ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

Str. Delea Nouă nr.2, Sector 3, 030925 Bucureşti, România
Telefon: 0372 845 400 / 0372 845 454. Fax: 0372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

În atenţia operatorilor economici interesaţi,

SOLICITARE DE OFERTE

Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii (ANCOM), cu sediul în Mun. Bucureşti, Str. Delea Nouă, Nr. 2, Sector 3, Cod poştal: 030925, intenţionează să achiziţioneze servicii de evaluare a vulnerabilităților informatice (cod CPV: 72820000-4)
Punct de contact: Departamentul Achiziții/Serviciul Achiziții Operaționale, Tel. 0372.845.582, Fax: 0372.845.402, în atenţia: Luminița Tararache, email: luminita.tararache@ancom.org.ro

Tip anunt: Achiziţie directă
Tip contract: Servicii

I. Obiectul achiziţiei: servicii de evaluare a vulnerabilităților informatice în cadrul proiectelor: „Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali" și ,,Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații" prin teste specifice de penetrare din interiorul și exteriorul infrastructurii de comunicații specifice acestora, luând în considerare designul, implementarea, utilizarea, mentenanța și dezvoltarea acestor sisteme.

Recomandările implementate în urma serviciilor de evaluare a vulnerabilităților informatice în cadrul proiectelor menționate mai sus vor fi introduse în ciclul de viață al procesului de dezvoltare a software-ului aferent acestora pentru a asigura securitatea aplicațiilor, a echipamentelor de comunicații, a sistemelor de calcul pe care aceste aplicații rulează și a datelor vehiculate de aceste aplicații.

Obiectiv:

Scopul proiectului este de a testa și evalua din punct de vedere al vulnerabilităților informatice două dintre sistemele importante aparținând ANCOM, și anume: "Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali" și "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații".

În timpul activităților de testare și evaluare se vor identifica și documenta vulnerabilități ale sistemelor informatice menționate mai sus în ceea ce privește:

- Autentificarea și autorizarea – mecanismele prin intermediul cărora utilizatorii sunt identificați, autentificați și autorizați să folosească funcțiile sistemului;

- Confidențialitatea datelor – măsurile implementate pentru a preveni accesarea datelor privind utilizatorii (nume, adrese, date de contact, nume utilizator etc.) și a datelor stocate și vehiculate prin intermediul celor două sisteme informatice, de către persoane neautorizate;

- Integritatea datelor - măsurile implementate pentru a asigura integritatea și a preveni pierderea, distrugerea sau furtul datelor stocate și vehiculate de cele două sisteme informatice;

- Disponibilitatea serviciului – aspecte ce privesc furnizarea neîntreruptă a serviciilor furnizate de cele două sisteme informatice;

- Respectarea politicilor și a practicilor de securitate – modul în care angajații companiei înțeleg și respectă politicile și practicile de securitate existente.

Prin testarea securității sistemelor "Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali" și "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații" se va asigura identificarea posibilelor vulnerabilități existente la nivelul sistemelor hardware, bazelor de date și aplicațiilor software încorporate, furnizând echipelor care asigură operarea, întreținerea și dezvoltarea acestora recomandări/informații destinate remedierii vulnerabilităților identificate.

Valoare estimată fără TVA: **126.380 lei**

II. Cerințe funcționale:

Durata: 60 (șaizeci) de zile lucrătoare de la data semnării contractului de către ambele părți. Acest termen va fi împărțit în trei etape distincte dupa cum urmează:

1. Pre-evaluare (Pre-assesment) – maxim 15 zile lucrătoare
2. Evaluare (Assesment) – maxim 25 zile lucrătoare
3. Post-evaluare (Post-assesment) – maxim 20 zile lucrătoare

Pe parcursul derulării contractului, ANCOM se obligă să transmită prestatorului toate datele și informațiile solicitate și considerate relevante pentru derularea contractului, în termen de maxim 5 (cinci) zile lucrătoare de la primirea solicitărilor din partea prestatorului. Acest termen trebuie avut în vedere de către ofertanți în calcularea termenul maxim de prestare a serviciilor care nu trebuie să fie mai mare de 60 (șaizeci) de zile lucrătoare de la data semnării contractului de către ambele părți.
În situația nerespectării de către ANCOM a termenelor în sarcina sa pentru furnizarea datelor și informațiilor solicitate, perioadele cu care se depășesc aceste termene nu vor fi incluse în termenul de prestare a serviciilor și nu vor putea fi solicitate penalități de întârziere în sarcina vreunei părți pentru aceste întârzieri.

Locul de prestare a tuturor serviciilor aferente contractului și de predare a livrabilelor sunt:

- Sediul central al autorității contractante din Municipiul București, Strada Delea Nouă, Nr. 2, Sector 3, Cod poștal: 030925.
- Direcția Regională București a autorității contractante din Municipiul București, Strada Lucian Blaga, Nr. 4, Sector 3, Cod Poștal 031072

Cheltuielile aferente transportului la locul de prestare al serviciilor cad în sarcina Prestatorului.

Termenul de realizare a contractului se consideră respectat în măsura în care au fost primite de către ANCOM toate livrabilele solicitate în cadul **pct.8** din **Anexa 1 - Caietul de sarcini -** la prezenta solicitare de oferte și a fost semnat procesul-verbal de acceptanță finală, fără obiecțiuni, până la expirarea termenului asumat.

III. Cerinţe minimale de calificare:

1. Certificat constatator/extras de registru - Ofertantanții vor prezenta, **în original sau copie legalizată sau copie lizibilă certificată de reprezentantul ofertantului cu menţiunea *„conform cu originalul*"**, certificat constatator/extras de registru, eliberat de Oficiul Registrului Comerţului de pe lângă Tribunalul competent teritorial, având înscrisă de către reprezentantul operatorului economic mentiunea - „Informatiile cuprinse în acest certificat sunt reale/actuale la data limita de depunere a ofertelor". Din certificatul constatator/extrasul de registru prezentat trebuie să rezulte obiectul de activitate al ofertantului. Obiectul contractului trebuie să aibă corespondent în CAEN din certificatul constatator emis de ONRC.
2. Declarație privind personalul de specialitate - Ofertantanții vor prezenta, **Declarație pe propria răspundere** a reprezentantului legal privind personalul de specialitate în conformitate cu **Anexa nr.2** la prezenta solicitare de oferte, însoțită în mod obligatoriu de diplome/certificate de absolvire și, **în original, declarație de disponibilitate**, semnată de fiecare persoană nominalizată.

3. Recomandări – ofertanții vor prezenta **recomandări** contrasemnate de beneficiari după cum urmează:

- pentru managerul de proiect - cel puțin o recomandare contrasemnată de beneficiar din care să reiasă că a participat în ultimii trei ani la un contract similar în calitate de manager de proiect
- pentru expert 1 Tester securitate aplicații software - recomandări contrasemnate de beneficiari din care să reiasă că a participat în ultimii trei ani la cel puțin trei contracte ca expert în testarea securității aplicațiilor WEB, a unui sistem informatic sau similar
- pentru expert 2 Consultant de securitate sisteme informatice - recomandări contrasemnate de beneficiari din care să reiasă că a participat în ultimii trei ani ca auditor tehnic sau consultant la cel puțin trei contracte în domeniul securității informației.

IV. Specificaţii tehnice/ funcţionale privind serviciile solicitate:

În cadrul ofertei se vor prezenta toate documentele solicitate la **pct. 7 - Anexa nr. 1-Caietul de sarcini** - la prezenta solicitare de oferte.

Cerințele impuse vor fi considerate ca fiind minime și obligatorii. În acest sens, orice ofertă prezentată, care se abate de la prevederile **Anexei nr.1- Caietului de sarcini**, va fi luată în considerare, dar numai în măsura în care Propunerea tehnică presupune asigurarea unui nivel calitativ superior cerințelor minime din Caietul de sarcini. Ofertele care conțin caracteristici tehnice ale serviciilor inferioare celor prevăzute în Caietul de sarcini vor fi considerate neconforme și vor fi respinse.

V. Modalitatea de prezentare a ofertei

Pentru a fi admişi în cadrul procedurii de atribuire, ofertanţii trebuie să depună următoarele documente:

A. Documente de calificare: Documentele solicitate în cadrul cap. III (*Cerinţe minimale de calificare*).

B. Oferta tehnică – Documentele solicitate în cadrul cap. IV.(Specificaţii tehnice/ funcţionale privind serviciile solicitate).

C. Oferta financiară, care va conţine preţul exprimat în lei, **fără TVA**. Preţul ofertat trebuie să includă toate costurile Prestatorului, directe şi indirecte, legate de prestarea serviciilor care fac obiectul prezentei achiziţii.

Preţul ofertat va fi ferm şi nu poate fi modificat pe toată perioada prestării serviciilor care fac obiectul prezentei achiziţii.

VI. Condiţii contract:

În ofertă se va preciza termenul de **prestare a serviciilor**, care nu trebuie să fie mai mare 60 (șaizeci) de zile lucrătoare de la data semnării contractului de către ambele părți.

Termenul de realizare a contractului se consideră respectat în măsura în care au fost primite de către ANCOM toate livrabilele solicitate în cadul **pct. 8** din **Anexa nr.1 - Caietul de sarcini -** la prezenta solicitare de oferte și a fost semnat procesul-verbal de acceptanță finală, fără obiecțiuni, până la expirarea termenului asumat.

Pentru depăşirea termenului asumat, prestatorul va datora penalităţi de întârziere de 0,15% din valoarea prezentei achiziții, fără TVA, pentru fiecare zi de întârziere în îndeplinirea corespunzătoare a oricărei obligaţii, penalităţi ce vor fi pretinse şi/sau deduse şi reţinute de către ANCOM din obligaţiile de plată a preţului, fără nicio formalitate prealabilă de punere în întârziere.

În cazul în care penalităţile de întârziere nu pot fi deduse din preţ, prestatorul are obligaţia de a le plăti în termen de maxim 10 (zece) zile de la solicitarea ANCOM.

Prestatorul garantează Achizitorului faptul că serviciile prestate şi/sau rezultatele acestora nu încalcă şi nu vor încălca în vreun fel drepturile vreunei terţe părţi.

Conditii de plată: Prestatorul va transmite factura la sediul ANCOM din Strada Delea Nouă, Nr. 2, Sector 3, Cod poştal 030925, Mun. București.

Plata pretului se va efectua numai după semnarea procesului-verbal de acceptanță finală, fără obiecțiuni, a rezultatelor serviciilor.

Plata se va efectua in baza facturii transmise de prestator, primita şi acceptata de ANCOM, si in conformitate cu prevederile art. 36 alin. (1) din O.U.G. nr. 34/2009 privind plata facturilor in perioada 24-31 a lunii.

În situatia în care factura este primită anterior sau la data semnării procesului-verbal de acceptanță finală, fără obiecțiuni, a rezultatelor serviciilor, plata se va efectua in termen de maxim 30 de zile de la această dată si in conformitate cu prevederile art. 36 alin. (1) din O.U.G. nr. 34/2009 privind plata facturilor in perioada 24-31 a lunii.

In situatia in care factura este primita dupa semnarea procesului-verbal de acceptanță finală, fără obiecțiuni, a rezultatelor serviciilor, ANCOM are dreptul de a efectua plata in termen de maxim 30 de zile de la data primirii facturii si in conformitate cu prevederile art. 36 alin. (1) din O.U.G. nr. 34/2009 privind plata facturilor in perioada 24-31 a lunii.

Nu se admite efectuarea de plati in avans sau plati partiale.

Plata se considera efectuata la data debitarii contului ANCOM.

VII. Criterii de adjudecare:

Va fi selectată oferta care îndeplineşte toate cerinţele solicitate prin prezenta şi care are preţul cel mai scăzut în Lei, fără TVA.

VIII. Informații suplimentare:

Ofertele pot fi transmise până la data de **02.09.2014, ora 17:00.**

astfel:

1. prin e-mail, la adresa luminita.tararache@ancom.org.ro sau

2. depunere la registratura sediului central ANCOM din Bucureşti, str. Delea Nouă, nr. 2, sector 3, cod poştal: 030925.

Relaţii suplimentare la numărul de telefon 0372-845.582; persoană de contact: Luminița TARARACHE.

Oferta se poate retrage şi modifica înainte de data limită de depunere a ofertei, respectiv 02.09.2014, ora 17:00.

Oferta transmisă/depusă la o altă adresă sau după data de 02.09.2014, ora 17:00, nu va fi luată în considerare.

În cazul în care oferta se depune direct sau prin poştă, operatorul economic trebuie să prezinte oferta în plic sigilat şi marcat cu denumirea/numele şi sediul/adresa operatorului economic. De asemenea, pe plicul se va menţiona „În atenţia Departamentului Achiziţii ANCOM/ Serviciul Achiziții Operaționale". 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 puţin până la data de 20.10.2014.

Solicitarea de oferte împreună cu **Anexa nr. 1- Caietul de sarcini** poate fi vizualizată în întregime şi pe pagina de internet a ANCOM la adresa www.ancom.org.ro, secțiunea Anunțuri/achiziții publice.

Anexa nr.1

CAIET DE SARCINI

Servicii de evaluare a vulnerabilităților informatice

Caietul de sarcini constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Cerințele impuse vor fi considerate ca fiind minime și obligatorii. În acest sens, orice ofertă prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare, dar numai în măsura în care Propunerea tehnică presupune asigurarea unui nivel calitativ superior cerințelor minime din Caietul de sarcini. Ofertele care conțin caracteristici tehnice ale serviciilor inferioare celor prevăzute în Caietul de sarcini vor fi considerate neconforme și vor fi respinse.

1. Obiectul procedurii de atribuire

Îl constituie achiziția de servicii de evaluare a vulnerabilităților informatice în cadrul proiectelor: „Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali" și ,,Sistem de colectare, prelucrare si raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații" prin teste specifice de penetrare din interiorul și exteriorul infrastructurii de comunicații specifice acestora, luând în considerare designul, implementarea, utilizarea, mentenanța și dezvoltarea acestor sisteme.

Recomandările implementate în urma serviciilor de evaluare a vulnerabilităților informatice în cadrul proiectelor menționate mai sus vor fi introduse în ciclul de viață al procesului de dezvoltare a software-ului aferent acestora pentru a asigura securitatea aplicațiilor, a echipamentelor de comunicații, a sistemelor de calcul pe care aceste aplicații rulează și a datelor vehiculate de aceste aplicații.

2. Obiectiv general:

Scopul proiectului este de a testa și evalua din punct de vedere al vulnerabilităților informatice două dintre sistemele importante aparținând ANCOM, și anume: "Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali" și "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații".

În timpul activităților de testare și evaluare se vor identifica și documenta vulnerabilitățile ale sistemelor informatice menționate mai sus în ceea ce privește:

- Autentificarea și autorizarea – mecanismele prin intermediul cărora utilizatorii sunt identificați, autentificați și autorizați să folosească funcțiile sistemului;
- Confidențialitatea datelor – măsurile implementate pentru a preveni accesarea datelor privind utilizatorii (nume, adrese, date de contact, nume utilizator etc) și a datelor stocate și vehiculate prin intermediul celor două sisteme informatice, de către persoane neautorizate;

- Integritatea datelor - măsurile implementate pentru a asigura integritatea și a preveni pierderea, distrugerea sau furtul datelor stocate și vehiculate de cele două sisteme informatice;
- Disponibilitatea serviciului – aspecte ce privesc furnizarea neîntreruptă a serviciilor furnizate de cele două sisteme informatice;
- Respectarea politicilor și a practicilor de securitate – modul în care angajații companiei înțeleg și respectă politicile și practicile de securitate existente.

3. Descrierea aplicațiilor care vor fi testate

a. „Aplicație online pentru compararea ofertelor de comunicații pentru utilizatorii finali" sau pe scurt - Veritel.ro, este o aplicație interactivă care realizează, pe baza opțiunilor introduse de utilizatori, analize comparative ale planurilor tarifare existente pe piață, oferind un clasament al celor mai avantajoase oferte din punct de vedere al prețului.

ANCOM a realizat acest portal de Internet care să permită compararea tarifelor și condițiilor oferite de furnizori, prin intermediul unei aplicații interactive. Furnizorii au obligația să introducă în baza de date a aplicației orice nouă ofertă comercială și orice modificare a unor oferte existente în termen de 4 zile lucrătoare de la data lansării sau a modificării acestora.

Dintre toate ofertele de telefonie și acces la Internet introduse de operatori în baza de date, Veritel.ro le alege pe acelea care respectă criteriile selectate de utilizator și care conțin cel puțin serviciile pentru care utilizatorul și-a estimat consumul. Sistemul ordonează lista ofertelor selectate, strict în ordinea crescătoare a prețului fiecărei oferte.

Pe baza informațiilor obținute utilizatorii sau potențialii utilizatori pot face o alegere în cunoștință de cauză, atât în ceea ce privește furnizorul, cât și în ceea ce privește o anumită ofertă de servicii.

b. "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații"

Acest sistem informatic asigură accesul facil al furnizorilor de rețele și servicii de comunicații electronice, precum și reprezentanților ANCOM la un instrument sigur și actualizat de raportare a informațiilor statistice. Aceasta este o aplicație unitară, care pune la dispoziție celor implicați în acest proces toate funcționalitățile printr-o aplicație web unică, la care accesul se face prin conexiune securizată. Sistemul permite următoarele acțiuni:

- colectarea online și/sau offline, validarea și înregistrarea datelor într-o bază de date relațională;
- prelucrarea informațiilor colectate, pentru a se putea asigura obținerea rapoartelor necesare;
- publicarea indicatorilor selectați în acest scop.

Arhitectura tehnică a sistemului este bazată pe standardul SOA – (Service Oriented Architecture) și are următoarele componente tehnice:

- soluție pentru colectarea datelor statistice, managementul și semnarea electronică a formularelor;
- soluție pentru proiectarea și execuția rapoartelor;
- soluție pentru arhivarea și managementul înregistrărilor digitale;

- soluție pentru managementul datelor.

4. Cerințe minime obligatorii

4.1. Introducere

Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) este instituția care protejează interesele utilizatorilor de comunicații din România, prin promovarea concurenței pe piața de comunicații, administrarea resurselor limitate, încurajarea investițiilor eficiente în infrastructură și a inovației. Pentru realizarea misiunii sale, ANCOM administrează mai multe platforme electronice, prin intermediul cărora se furnizează servicii ce asigură schimbul de informații rapid și eficient cu operatorii de comunicații și alți terți aflați în relație cu instituția.

Prin testarea securității sistemelor "Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali" și "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații" se va asigura identificarea posibilelor vulnerabilități existente la nivelul sistemelor hardware, bazelor de date și aplicațiilor software încorporate, furnizând echipelor care asigură operarea, întreținerea și dezvoltarea acestora recomandări/informații destinate remedierii vulnerabilităților identificate.

Testele de penetrare "pentest" reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităților existente și cunoscute. Procesul implică o analiză activă a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvată și din breșe cunoscute sau necunoscute, hardware și software.

Scopul testelor de penetrare este acela de a analiza comportamentul sistemelor informatice menționate în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Un test de penetrare complet va cuprinde atât teste automate cât și manuale. Testele automate vor identifica erori de programare în aplicațiile utilizate și vor fi efectuate cu ajutorul unor programe specializate (vulnerability scanners, fuzzers, code scanners, etc). Testele manuale vor analiza aspecte ale aplicațiilor care necesită intuiția umană, identificându-se erori logice de programare și vor analiza și confirma sau infirma rezultatele testelor automate.

4.2 Evaluarea posibilelor vulnerabilități vizibile atât din interiorul cât și din exteriorul rețelei ANCOM

Tipul testării, roluri și scenarii de atac

Testele de penetrare (pentest) vor avea ca și rezultat o analiză complexă a securității sistemelor informatice menționate, testând eficacitatea măsurilor de securitate implementate prin simulare unor atacuri informatice. Activitățile echipei de testare se vor baza pe practici de "ethical hacking", iar posturile pe care le va lua echipa vor fi următoarele:

A. Black box – în această situație echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția numelor aplicațiilor (adresa web) sau a unor adrese IP.

În cadrul acestui tip de testare se va evidenția un singur rol, și anume:

- Utilizatorul anonim, cu următoarele caracteristici:
  - nu are drepturi sau privilegii;
  - nu are cont de utilizator;
  - nu deține informații despre sistemele informatice;
  - deține informații disponibile public referitoare la sistemele testate.

B. White box – echipa de testare va avea acces la orice informație despre sisteme, incluzând codul sursă sau privilegii administrative. În timpul acestei testări se va simula o activitate care să reflecte ceea ce s-ar putea întâmpla în timpul unor activități rău voitoare și nelegitime, în cazul în care atacatorul are acces la codul sursă, machetele de rețea și, eventual, chiar la unele parole.

În cadrul acestui tip de testare se vor identifica următoarele roluri:

- Pentru „Aplicație online pentru compararea ofertelor de comunicații destinate utilizatorilor finali - VERITEL”:

I.1. Administrator sistem: deținător de drepturi de administrare sistem:
- este deținător de cont (username şi parolă);
- atacul se va executa din Internet.

I.2. Utilizator public cu cont (username și parolă):
- atacul se va executa din Internet.

I.3. Utilizator individual – deținător de cont (username și parolă):
- are drepturi și acces la funcționalitățile de bază ale aplicației;
- atacul se va executa din Internet.

I.4. Utilizator privilegiat – deținător de drepturi de administrare a unui număr limitat de utilizatori externi:
- este deținător de cont (username și parolă);
- atacul se va executa din Internet.

I.5. Operator telecom subordonat – „editor”
- are drepturi limitate la introducerea de date din postura unui operator telecom;
- este deținător de cont (username și parolă);
- atacul se va executa din Internet.

I.6. Operator telecom privilegiat – „administrator”
- are drepturi de management asupra unui număr restrâns de utilizatori subordonați de tip „editor”:
- este deținător de cont (username și parolă);
- atacul se va executa din Internet.

- Pentru “Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații”:

II.1. Administrator sistem: deținător de drepturi de administrare sistem:
- este deținător de cont (username și parolă);
- atacul se va executa din Internet.

II.2. Administrator

- Sunt utilizatorii interni ce au următoarele atribuții: Managementul utilizatorilor interni și externi etc;
- atacul se va executa din Internet.

II.3. Proiectant Anchetă

- Sunt utilizatorii interni ce au cunoștințe pentru a defini, proiecta și testa formularele statistice;
- atacul se va executa din Internet.

II.4. Statistician

- Sunt utilizatori interni ce au atribuții în a supraveghea modul în care furnizorii de date completează formularele statistice;
- atacul se va executa din Internet.

II.5. Supervizor

- Sunt utilizatori interni ce au atribuții în a supraveghea modul în care toți furnizorii de date completează formularele statistice;
- atacul se va executa din Internet.

La aceste conturi definite se vor adăuga cel mult încă alte 2(două) conturi ce vor fi identificate pe parcursul desfășurării testărilor.

4.3. Desfășurarea proiectului

4.3.1. În cadrul proiectului se solicită oferirea următoarelor servicii:

- servicii de testare din punct de vedere al securității - PEN TEST - pentru cele două sisteme aparținând ANCOM - "Aplicație online pentru compararea ofertelor de comunicații pentru utilizatorii finali" și "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații";
- servicii de documentare a proiectului.

4.3.2. Planificarea și graficul activităților

- Ofertantul va prezenta planificarea activităților propuse, precum și interdependența acestora. Planul trebuie să menționeze care sunt termenele cheie (milestones) pe care ofertantul și le-a propus să le respecte pentru atingerea obiectivelor. Planul va fi prezentat sub forma unui grafic de proiect (exemplu: tip Gantt).
- Graficul planificării activităților proiectului va trebui să fie particularizat pentru proiect și să conțină alocarea resurselor.

4.3.3. Furnizorul va lua toate măsurile necesare astfel încât pe perioada desfășurării activităților de detectare și evaluare a vulnerabilităților pentru "Aplicație online pentru compararea ofertelor de comunicații pentru utilizatorii finali" și "Sistem de colectare, prelucrare și raportare a datelor statistice aferente furnizorilor de servicii de telecomunicații", sistemele informatice ale ANCOM impactate de desfășurarea testelor nu vor întâmpina probleme care să ducă la blocarea proceselor curente de lucru ale ANCOM sau la pierderi de date și/sau informații.

5. Etape pentru desfășurarea serviciilor de evaluare

Evaluarea și testarea se vor derula prin intermediul a trei etape distincte, și anume:

- Pre-evaluare (Pre-assesment)
- Evaluare (Assesment)
- Post-evaluare (Post-assesment)

5.1 Pre-evaluare (Pre-assesment)

Reprezintă faza premergătoare evaluării vulnerabilităților și este importantă pentru determinarea specificațiilor precise și regulilor de desfășurare a evaluării.

În această etapă se vor stabili și elabora planul de proiect detaliat, planul de testare, planul de acțiuni (SOW – State of Work) precum și scenariile de atac și se vor obține autorizațiile necesare desfășurării testelor de penetrare.

Această etapă se va desfășura pe parcursul a maximum 15 zile lucrătoare și se va finaliza cu elaborarea Planului de proiect dealiat, a Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor înscrie cel puțin: activitățile convenite, sistemele incluse în activitatea de testare, termenul propus de realizare, termenul efectiv de realizare, persoane responsabile atât din partea beneficiarului, cât și a prestatorului.

5.2 Evaluare (Assesment)

Reprezintă etapa de evaluare a vulnerabilităților de securitate ale celor două sisteme informatice.

Această fază a testării include evaluarea conectivității între sistemele utilizate pentru test și sistemele testate, culegerea informațiilor despre sistemele testate din domeniul public și privat, descoperirea sistemelor și serviciilor active precum și scanarea sistemelor pentru descoperirea vulnerabilităților.

Utilizând informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac (attack trees) și se vor implementa acțiunile definite în aceste structuri.

Scanarea vulnerabilităților și implementarea testului de penetrare va include, dar nu se va limita la analiza următoarelor vulnerabilități ale aplicațiilor web:

- Verificarea input-ului utilizatorului;
- Controlul accesului;
- Cross Site Scripting (XSS) ;
- Buffer overflow;
- Tratarea erorilor;
- Injectare de cod arbitrar;
- Criptarea și stocarea informației în execuția aplicației;
- Erori de configurare a aplicației.

Scanarea vulnerabilităților și implementarea testului de penetrare la nivelul rețelei va include dar nu se va limita la :

- Obținerea informațiilor din domeniul public;
- Scanarea sistemelor din SOW;
- Tehnici de enumerare;
- Obținerea accesului neautorizat prin exploatarea vulnerabilităților;

- Consolidarea accesului;
- Ștergerea tuturor fișierelor utilizate în cadrul atacului și a altor dovezi ale accesului.

Aplicații software utilizate în cursul testării:

- Aplicații pentru culegerea de informații din domeniul public;
- Aplicații necesare identificării sistemelor și serviciilor active;
- Scannere de vulnerabilități specifice sistemelor și rețelelor incluse în Planul de acțiuni (SOW - State of Work);
- Aplicații necesare exploatării vulnerabilităților descoperite.

Această etapă se va desfășura pe parcursul a maximum 25 de zile lucrătoare și se va finaliza cu elaborarea de către prestator a două rapoarte de test (câte unul pentru fiecare din cele două sisteme testate) care vor include toate problemele și vulnerabilitățile descoperite pe parcursul testării.

5.3 Post-evaluare (Post-assesment)

Reprezintă etapa de analiză a problemelor și vulnerabilităților descoperite în etapa de Assesment.

Această etapă se va desfășura pe parcursul a maximum 20 de zile lucrătoare și se va finaliza cu elaborarea de către prestator a două rapoarte de analiză a rezultatelor testelor efectuate in care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact.

În această etapă prestatorul va acorda suport beneficiarului pentru înțelegerea deplină a problemelor identificate și alegerea măsurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite.

6. ALTE CERINŢE MINIME OBLIGATORII

Prestatorul trebuie să poată identifica și evalua vulnerabilitățile informatice care să adreseze cel puțin următoarele concepte și tipuri de atac:

- RFI – Remote File Inclusion;
- LFI – Local File Inclusion;
- XSS – Cross Site Scripting;
- HTTP Header Injection;
- SQL Injection;
- LoginByPass – evitarea autentificării;
- Arbitrary File Upload;
- Remote Code and Command Execution;
- Full Path Disclosure;
- Metodele nesigure de utilizare a cookie-urilor;
- Cross Site Request Forgery;
- Directory Traversal;
- HTTP Parameter Pollution;
- Script Source Code Disclosure;

- CRLF Injection;
- XFS - Cross Frame Scripting;
- PHP Code Injection;
- XPath Injection;
- LDAP Injection;
- Email Injection;
- Arbitrary File Creation;
- File Tampering;
- Remote XSL Inclusion;
- MultiRequest Parameter Manipulation;
- Input Validation;
- Buffer Overflows;
- Unrestricted File Uploads.

Prestatorul va descoperi eventualele vulnerabilităţi de securitate existente cel puțin în cadrul:
- Paginilor Web caracteristice protocoalelor SSL/TLA;
- Paginilor Web caracteristice protocolului HTTPS;
- Paginilor Web care să adreseze conceptul de Directory Checks;
- Paginilor Web care să adreseze conceptul de Text Search;
- Aplicaţiei OWA – Outlook Web Application;
- Reţelelor de comunicaţii legate de protocolul SNMP;
- Rețelelor de comunicații legate de protocolul TCP/IP;
- Rețelelor de comunicații legate de protocolul LDAP;
- Rețelelor de comunicații legate de tehnologia DNS;
- Rețelelor de comunicații legate de protocolul TELNET;
- Rețelelor de comunicații legate de protocolul SSH;
- Rețelelor de comunicații legate de metodele de autentificare utilizate – weak passwords, default passwords, etc;
- Rețelelor de comunicații legate de protocolul ARP;
- Rețelelor de comunicații legate de protocolul UDP;
- Rețelelor de comunicații legate de protocolul SMTP;
- Rețelelor de comunicații legate de protocolul FTP;
- Rețelelor de comunicații legate de funcționalitățile NetBIOS;
- Reţelelor de comunicații legate de funcționalitățile Microsoft RDP.

Alte vulnerabilități vor fi evidențiate prin:
- Analiza sintaxei parolelor și a posibilelor puncte slabe ale acestora (Weak Password Check) – weak HTTP password, authentication attacks, weak FTP passwords;

- Scanarea porturilor/rețelei – Open Ports on Servers, Network Banner of port, DNS Server Vulnerability – Open Zone Transfer, Open Recursion, Cache Poisoning, List of writable FTP Directories, FTP Anonymous Access Allowed, Badly Configured Proxy Servers, Weak SNMP Community Strings, Weak SSL Cyphers);

Soluția propusă va identifica cel puțin majoritatea vulnerabilităților prezente în următoarele baze de date: CVE (Common Vulnerabilities and Exposures), CWE (Common Weakness Enumeration), CCE (Common Configuration Enumeration), Bugtraq (SecurityFocus).

7. Conținutul ofertei:

7.1 Ofertantul va prezenta, **în original sau copie legalizată sau copie lizibilă certificată de reprezentantul ofertantului cu mențiunea *„conform cu originalul”***, certificat constatator/extras de registru, eliberat de Oficiul Registrului Comerțului de pe lângă Tribunalul competent teritorial, având înscrisă de către reprezentantul operatorului economic mențiunea - „Informațiile cuprinse în acest certificat sunt reale/actuale la data limita de depunere a ofertelor”. Din certificatul constatator/extrasul de registru prezentat trebuie să rezulte obiectul de activitate al ofertantului. Obiectul contractului trebuie să aibă corespondent în CAEN din certificatul constatator emis de ONRC.

7.2 Standarde de asigurare a calității și de protecția mediului

Prestatorul trebui să demonstreze că are implementate:

a) Sistem de Management al calității în conformitate cu prevederile SR EN ISO 9001 sau echivalent, prin prezentarea unor documente edificatoare, în copie lizibilă certificată de reprezentantul ofertantului cu mențiunea „conform cu originalul”, care să ateste că are implementat un sistem de management al calității în conformitate cu prevederile SR EN ISO 9001 sau echivalent, valabile la data limită de depunere a ofertelor.

b) Sistem de Management al Securității Informației în conformitate cu prevederile SR ISO/CEI 27001 sau echivalent, prin prezentarea unor documente edificatoare, în copie lizibilă certificată de reprezentantul ofertantului cu mențiunea „conform cu originalul”, care să ateste că are implementat un Sistem de Management pentru Securitatea Informației în conformitate cu prevederile SR ISO/CEI 27001 sau echivalent, valabile la data limită de depunere a ofertelor.

7.3 Oferta va menționa metodologiile, tehnicile și standardele utilizate în evaluarea vulnerabilităților (spre exemplu NIST – National Institute of Standards and Technology, OSSTM - Open Source Security Testing Methodology, ISACA – Information Systems Audit and Control Association, ISSAF – Information Systems Security Assessment Framework) și o scurtă prezentare a acestora.

Prestatorul va atașa ofertei modele de documente care să descrie livrabilele aferente proiectului, modele care vor respecta cerințele din prezentul caiet de sarcini.

7.4 Echipa de proiect

Ofertantul va prezenta informații referitoare la personalul de specialitate din care trebuie să rezulte că dispune sau a obținut angajamentul de participare pentru cel puțin 3 (trei) specialiști și că persoanele nominalizate au experiența profesională și cunoștințele teoretice și practice relevante menționate în cele ce urmează.

7.4.1 Manager de Proiect – 1 (una) persoană – care trebuie să îndeplinească următoarele cerințe:

a. cunoștințe aprofundate în domeniul managementului de proiect în ceea ce privește conceptele, tehnicile, principiile, metodele și metodologiile de management de proiect, într-un mod standardizat. Se va face dovada absolvirii, de către persoana nominalizată, a cel puțin un curs de management de proiect, ITIL sau echivalent;
b. certificare specifică în domeniul managementului securității informației (CISA, CISM, CISSP sau echivalent);
c. participarea în ultimii trei ani la un contract similar în calitate de manager de proiect.

7.4.2. Expert 1 Tester securitate aplicații software - 1 (una) persoană – care trebuie să îndeplinească următoarele cerințe:

a. certificare, care să ateste cunoștințe în testarea securității aplicațiilor software (CEH, LPT sau echivalent);
b. certificare în domeniul de dezvoltare aplicații software (Microsoft, Oracle sau echivalent);
c. certificare specifică în domeniul managementului securității informației (CISA, CISM, CISSP sau echivalent);
d. participarea în ultimii trei ani la cel puțin trei contracte ca expert în testarea securității aplicațiilor WEB, a unui sistem informatic sau similar.

7.4.3. Expert 2 Consultant de securitate sisteme informatice - 1 (una) persoană - care trebuie să îndeplinească următoarele cerințe:

a. certificare care să ateste cunoștințe privind standardele și bunele practici în domeniul securității informației (ISO 27001 sau echivalent);
b. certificare care să ateste cunoștințe privind auditul, managementul securității informației (ISO 27001 Lead Auditor, CISA sau echivalent);
c. participarea în ultimii trei ani ca auditor tehnic sau consultant la cel puțin trei contracte în domeniul securității informației.

Pentru a demonstra îndeplinirea cerințelor de mai sus privind echipa de proiect, ofertantul va prezenta, în original, **Declarație pe propria răspundere** a reprezentantului legal privind personalul de specialitate în conformitate cu **Anexa nr.2** la prezentul caiet de sarcini, însoțită în mod obligatoriu de diplome/certificate de absolvire și, în original, declarație de disponibilitate, semnată de fiecare persoană nominalizată. Totodată ofertantul va prezenta recomandări contrasemnate de beneficiari după cum urmează:

- pentru managerul de proiect - cel puțin o recomandare contrasemnată de beneficiar din care să reiasă că a participat în ultimii trei ani la un contract similar în calitate de manager de proiect

- pentru expert 1 Tester securitate aplicații software - recomandări contrasemnate de beneficiari din care să reiasă că a participat în ultimii trei ani la cel puțin trei contracte ca expert în testarea securității aplicațiilor WEB, a unui sistem informatic sau similar
- pentru expert 2 Consultant de securitate sisteme informatice - recomandări contrasemnate de beneficiari din care să reiasă că a participat în ultimii trei ani ca auditor tehnic sau consultant la cel puțin trei contracte în domeniul securității informației.

8. Livrabile

Livrabilele vor include în mod obligatoriu:

- Plan de proiect detaliat;
- Plan de testare;
- Planul de acțiuni (SOW – State of Work);
- Două rapoarte de test (câte unul pentru fiecare din cele două sisteme testate) care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor;
- Două rapoarte de analiză (câte unul pentru fiecare din cele două sisteme testate), conținând analiză a rezultatelor testelor efectuate in care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate.

Rapoartele furnizate de prestator vor fi structurate în două părți distincte: partea executivă și partea tehnică. Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice (cel puțin diagrame, grafice sau harți). Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate.

Partea tehnică va conține cel puțin următoarele capitole:

- Sumar executiv;
- Obiectivele și scopul evaluării;
- Prezentare succintă a metodologiei utilizate în cadrul testării;
- Descrierea contextului în care s-a desfășurat testarea;
- Prezentarea individuală a vulnerabilităților descoperite, după cum urmează:
    - descrierea vulnerabilității;
    - catalogarea vulnerabilității;
    - descrierea tehnică;
    - analiza severității și probabilității;
    - calcularea riscului;
    - contramăsuri recomandate pentru remediere.
- Alte detalii și recomandări;
- Anexa cu lista testelor de securitate efectuate.

Recomandările de remediere a problemelor și vulnerabilităților identificate vor cuprinde cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului

generat de problemele și vulnerabilitățile detectate precum și recomandări și propuneri de implementare ale acestora.

9. Termenul de realizare a contractului

Termenul de realizare a contractului este de maximum 60 (șaizeci) de zile lucrătoare de la data semnării contractului de către ambele părți.

Termenul de realizare a contractului se consideră respectat în măsura în care au fost primite de către ANCOM toate livrabilele solicitate în cadrul **pct.8** din prezentul Caiet de sarcini și a fost semnat procesul-verbal de acceptanță finală, fără obiecțiuni, până la expirarea termenului asumat.

10. Pe parcursul derulării contractului, ANCOM se obligă să transmită prestatorului toate datele și informațiile solicitate și considerate relevante pentru derularea contractului, în termen de maxim 5 (cinci) zile lucrătoare de la primirea solicitărilor din partea prestatorului. Acest termen trebuie avut în vedere de către ofertanți în calcularea termenului maxim de prestare a serviciilor care nu trebuie să fie mai mare de 60 (șaizeci) de zile lucrătoare de la data semnării contractului de către ambele părți.

În situația nerespectării de către ANCOM a termenelor în sarcina sa pentru furnizarea datelor și informațiilor solicitate, perioadele cu care se depășesc aceste termene nu vor fi incluse în termenul de prestare a serviciilor și nu vor putea fi solicitate penalități de întârziere în dauna vreunei părți pentru aceste întârzieri.

11. Marca, modelul și producătorul produselor

Se vor specifica denumirile, versiunile și producătorii pachetelor software care se vor folosi pe parcursul derulării contractului; de asemenea se vor atașa documente de la producători în copie (file de catalog, prospecte, etc.) care să conțină caracteristicile produselor folosite. Se admite ca aceste documente să fie prezentate în limba engleză.

Prestatorul își va asuma răspunderea legalității utilizării instrumentelor folosite în cadrul proiectului. ANCOM își rezervă dreptul de a solicita dovada utilizării legale a acestora.

12. Livrare

Locul de prestare a tuturor serviciilor aferente contractului sunt:

- Sediul central al autorității contractante din Municipiul București, Strada Delea Nouă, Nr. 2, Sector 3, Cod poștal: 030925.
- Direcția Regională București a autorității contractante din Municipiul București, Strada Lucian Blaga, Nr. 4, Sector 3, Cod Poștal 031072

Cheltuielile aferente transportului la locul de prestare al serviciilor cad în sarcina Prestatorului.

Anexa nr. 2

OFERTANT,

_____

(denumirea/numele)

DECLARAŢIE
privind personalul de specialitate

Subsemnatul(a) _____, reprezentant legal/ împuternicit al _____ *(denumirea/numele şi sediul/adresa operatorului economic)*, în calitate de ofertant la procedura de achiziție directă de servicii de evaluare a vulnerabilităților informatice (cod CPV: 72820000-4), organizată de Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, declar pe propria răspundere, sub sancţiunea excluderii din procedura de atribuire şi a sancţiunilor aplicate falsului în declaraţii, că _____ (*denumirea/numele operatorului economic*) dispune de personal de specialitate conform cerințelor din caietul de sarcini:

- în calitate de **manager de proiect**, dl./dna……., date de contact……..
- în calitate de **expert 1** Tester securitate aplicații software, dl./dna……., date de contact……..
- în calitate de **expert 2** Consultant de securitate sisteme informatice, dl./dna……., date de contact……..

Totodată, anexez prezentei declarații documentele solicitate pentru fiecare persoană menționată mai sus astfel cum s-a solicitat în cadrul pct. 7.4 din Anexa 1 - Caietul de sarcini.

Subsemnatul(a) declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi înteleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, situaţiilor şi documentelor care însoţesc oferta, orice informaţii suplimentare în scopul verificării datelor din prezenta declaraţie.

Subsemnatul(a) declar că în situaţia în care ..... (*denumirea/numele operatorului economic)* va fi desemnat câştigător al prezentei proceduri de atribuire, se va asigura prestarea tuturor serviciilor care fac obiectul achiziţiei prin personalul menţionat în prezenta declaraţie pe propria răspundere.

Data completării _____.

OFERTANT,