Caiet de sarcini

privind serviciilor de evaluare și de analiză a asigurării calității sistemelor (servicii de testare a securității sistemului informatic al Procuraturii Generală, Procuraturilor specializate și teritoriale)

Nr. d/o	Cod CPV	Denumirea serviciilor	Un. de măs.	Can ti-tate a	Specificarea tehnică deplină solicitată, Standarde de referință, Cerințe față de serviciile achiziționate
1	72212900-8	Servicii de testare a securității sistemului informatic al Procuraturii (Procuratura Generală, procuraturile specializate și teritoriale)	buc	1	**1.1. Obiectul achiziției** Obiectul achiziției reprezintă contractarea serviciilor de penetrare și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic (SI) al Procuraturii Republicii Moldova prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea care vor include: - Penetration testing a infrastructurii expuse în internet, inclusiv aplicațiile; - Penetration testing a infrastructurii expuse în rețeaua procuraturii, inclusiv aplicațiile; - Evaluarea vulnerabilității (vulnerability assessment) infrastructurii de rețea inclusiv infrastructura wireless (dacă există) și penetrarea ei. Testele de penetrare reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităților existente și cunoscute într-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența că acestea vor fi efectuate într-un mod etic, cu permisiunea Beneficiarului. 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. Prin testarea securității sistemelor informatice se va asigura identificarea posibilelor vulnerabilități existente la nivelul sistemelor hardware, bazelor de date și aplicațiilor software încorporate, furnizînd echipelor, care asigură operarea, întreținerea și dezvoltarea acestora, informații și recomandări destinate remedierii vulnerabilităților identificate. **1.2. Scopul serviciilor prestate** 1.2.1. Scopul testelor de penetrare este de a analiza comportamentul sistemelor informatice în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Un test de penetrare complet va cuprinde atît teste automate cît și manuale. - *Testele automate* vor identifica erori de programare în aplicațiile utilizate și vor fi efectuate cu ajutorul unor programe specializate precum instrumentele de scanare a vulnerabilităților, a aplicațiilor web și a codului, instrumente de testare și identificare a eventualelor erori de programare din aplicații în vederea exploatării lor. - *Testele manuale* vor analiza aspecte ale aplicațiilor care necesită intuiția umană, identificîndu-se erori logice de programare, și vor analiza și confirma sau infirma rezultatele testelor automate. Pentru atingerea acestor obiective, serviciile de penetrare si evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Procuraturii prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea urmează să fie prestate de Ofertantul selectat conform cerințelor stabilite în acest caiet de sarcini. 1.2.2. Ofertantul trebuie să descrie activitățile ce vor fi desfășurate de acesta pentru a răspunde acestor cerințe. Ofertantul trebuie să prezinte informație despre modul în care intenționează să presteze serviciile solicitate la nivelul cerut, precum și informație privind capacitățile sale tehnice,

					organizatorice și de competența, ce confirmă capacitatea sa de a presta la nivelul cerut. **1.3. Cerințele față de serviciile de penetrare** 1.3.1. Serviciile de penetrare vor avea ca rezultat o analiză complexă a securității sistemelor informatice ale Beneficiarului, testînd eficacitatea măsurilor de securitate implementate prin simularea 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 informației de accesare a aplicațiilor (pagini web, adrese IP). Această metodă va fi utilizată pentru testarea infrastructurii externe a Beneficiarului. 1.3.2. Ofertantul va trebui să utilizeze echipamente și aplicații, și să dețină experiență pentru realizarea de teste de penetrare la nivel de rețea, inclusiv wireless, sistem de operare, baze de date și aplicații, inclusiv cele web, atacuri informatice simulînd aplicații malițioase, cît și de negare a serviciului (DoS). 1.3.3. Ofertantul va trebui să dețină și să utilizeze echipamente și aplicații dedicate pentru identificarea și obținerea informațiilor despre sistemele informatice țintă, identificarea de vulnerabilități, și formularea unor recomandări de remediere. 1.3.4. Ofertantul va trebui să dețină proceduri de lucru conforme standardelor în domeniu, prin care este redus riscul de a afecta sistemele informatice aflate în scopul testării. **1.4. Cerințe față de etapele procedurii de evaluare și testare.** Serviciile de penetrare și evaluare a vulnerabilităților informatice în cadrul SI al Procuraturii Republicii Moldova prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea se vor derula în trei etape distincte, și anume: *1. Pre-evaluare (Pre-assesment)* *2. Evaluare (Assesment)* *3. Post-evaluare (Post-assesment)* 1.4.1. ***Etapa de Pre-evaluare (Pre-assesment)*** - reprezintă faza premergătoare evaluării vulnerabilităților și este importantă pentru determinarea specificațiilor precise și a regulilor de desfășurare a evaluării. În această etapă se vor stabili și elabora 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 numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor înscrie cel puțin: - activitățile întreprinse, - sistemele incluse în activitatea de testare, - termenul propus de realizare, - persoane responsabile atît din partea Beneficiarului, cît și a Prestatorului. 1.4.2. ***Etapa de Evaluare (Assesment)*** - reprezintă etapa de identificare și evaluare a vulnerabilităților de securitate a sistemelor informatice. Această etapă 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.

					Utilizînd informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac 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: • Injectarea de cod malițios • Managementul defectuos al procesului de autentificare și al sesiunii de lucru • Cross-Site Scripting (XSS) • Referențierea directă a obiectelor în mod nesecurizat • Erori privind configurația de securitate • Tratarea erorilor în mod nesecurizat și lipsa de măsuri de protecție a informațiilor sensibile • Controale ineficiente privind managementul accesului • Cross-Site Request Forgery (CSRF) • Utilizarea de componente de sistem cu vulnerabilități cunoscute • Validarea parametrilor de intrare ai aplicațiilor • Comportamentul aplicațiilor/sistemelor aflate în scop la un atac de tip Denial of Service (DoS) În privința managementului sesiunii de lucru se vor identifica cel puțin următoarele aspecte: • Implementarea managementului sesiunii printr-un Framework cunoscut și de încredere, care a fost testat în practică din punct de vedere al securității. • Procesul de generare a identificatorilor de sesiune și protecția acestora împotriva abuzurilor. • Procesul de generare a cookie-urilor ce conțin generatori de sesiune și stabilire a atributelor acestora. • Procesul de creare și terminare a sesiunii și identificatorilor din perspectiva server și client. • Intervaluri de inactivitate și posibilitatea de inițializare de multiple sesiuni active. • Măsurile implementate pentru păstrarea confidențialității informațiilor privind autentificarea și sesiunea de lucru. • Implementarea de măsuri adiționale de securitate pentru operațiile sensibile, precum cele administrative. În privința configurației de securitate se vor identifica cel puțin următoarele aspecte: • Versiunile de software ale serverelor, platformelor de dezvoltare a aplicației și componentelor sistemului. • Existența actualizărilor de securitate aflate pe serverele, platformele de dezvoltare a aplicației și componentele sistemului. • Existența configurațiilor prestabilite de la producătorul sistemului, cum ar fi utilizatori și parole implicite. • Utilizatorii de aplicații și configurația acestora. • Metodele și extensiile protocolului HTTP folosite în cadrul sistemului. • Informații relevante ce se afla în header-ul HTTP. • Existența mecanismelor de criptare pentru autentificarea în cadrul sistemelor și transmisia de informații. În privința tratării erorilor de sistem și protejării informațiilor sensibile se vor identifica cel puțin următoarele aspecte: • Identificarea posibilității ca aplicațiile să divulge informații sensibile, inclusiv detalii despre sistem, identificatori de sesiune sau informații despre cont, în mesaje de erori. • Conținutul mesajelor de eroare din punct de vedere tehnic. În privința managementului accesului se vor identifica cel puțin următoarele aspecte:

					• Procesul de identificare, autentificare si autorizare a accesului la informații. • Identificarea credențialelor hard-codate în sisteme, dacă acestea există. • Identificarea utilizatorilor și credențialelor de acces stocate în fișiere de configurație în clar. • Identificarea credențialelor transmise in clar, daca este cazul. • Identificarea rolurilor de acces și maparea acestora pe drepturi și posibilitatea de ocolire a acestora pentru a obține acces neautorizat la informații. • Identificarea metodelor HTTP folosite în procesul de autentificare. În privința validării parametrilor de intrare se vor identifica cel puțin următoarele aspecte: • Filtrarea și validarea datelor provenite din afara sistemelor • Existența unei metode centralizate de validare a datelor în sistem. • Existența unor seturi de caractere corespunzătoare pentru datele de intrare • Codificarea datelor într-un set comun de caractere înainte de validare • Validarea datelor provenite de la utilizatori, înainte de procesarea acestora, inclusiv toți parametrii, conținutul URL si HTTP. Pentru validarea datelor de intrare se vor verifica: • tipurile de date așteptate (integer, string etc,) • setul de date • lungimea datelor • Implementarea de măsuri suplimentare de control pentru caractere cu potențial riscant (< > " ' % ( ) & + \ \' \") Testarea securității la nivelul infrastructurii Wi-Fi va include, dar nu se va limita la : • Descoperirea rețelelor Wi-Fi și punctelor de acces atît cunoscute cît și neautorizate • Identificarea dispozitivelor care interacționează cu rețeaua • Colectarea de informații despre puterea de rețea, protocoale de securitate și a dispozitivelor conectate • Atacul și penetrarea rețelelor criptate cu WEP, WPA-PSK si WPA2-PSK • Impersonare SSID • Atacuri de tip Man-in-the-middle (MITM) • Monitorizare automată trafic pentru a găsi fluxuri de date sensibile • Aderarea la rețelele compromise și testarea sistemelor de backend • Raportare cuprinzătoare a activităților de testare a rețelelor de tip Wi-Fi 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. Prin testarea automată va trebui să se detecteze cel puțin următoarele tipuri de vulnerabilități:

					• Parole inițiale neschimbate pe echipamente • Posibilitatea de acces în sistem fără autentificare, cu autentificare cu credențiale inițiale sau credențiale ușor de ghicit • Configurații inițiale neschimbate pe echipamente • Corecții și actualizări de securitate neimplementate • Escaladarea privilegiilor • Software cu versiuni vechi și foarte vechi ce prezintă vulnerabilități • Buffer Overflow • Negarea accesului la serviciu (DoS Denial of Service) • Remote Code Execution • Posibilitatea injectării de comenzi sau scripturi în servere web, servere de aplicații și baze de date • Directory Traversal • File and Path Disclosure • Cross Site Scripting (XSS) • Cross Site Request Forgery (CSRF) • Configurarea defectuoasă a serverelor • Managementul defectuos al sesiunilor și autentificării • Parametri de intrare nevalidați • Control al accesului defectuos • Tratarea defectuoasă a erorilor Soluția de testare automată utilizată trebuie să fie capabilă să integreze capabilitățile de descoperire și remediere a vulnerabilităților cu informații despre *aplicațiile malware* prezente în infrastructură, cît și toate aplicațiile malware cunoscute cu ajutorul cărora se pot exploata vulnerabilitățile prezente și ușurința cu care aceste vulnerabilități se pot exploata. Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de test care vor include toate problemele și vulnerabilitățile descoperite pe parcursul testării. 1.4.3. ***Etapa de Post-evaluare (Post-assesment)*** - această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de analiză, a rezultatelor testelor efectuate în 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. Totodată Prestatorul va efectua test de penetrare repetat la resursele cu probleme identificate pentru a verifica daca au fost aplicate corect măsurile/metodele de remediere. **1.5. Cerințe față de livrabilele proiectului** Ca urmare a serviciilor prestate, Ofertantul selectat va oferi cel puțin următoarele livrabile: • Plan de proiect; • Plan de testare; • Planul de acțiuni (SOW – Scope of Work); • Rapoarte de test care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor; • Rapoarte de analiză, ce vor conține analiza rezultatelor testelor efectuate prin 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. *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; • Prezentarea metodologiei utilizate în cadrul testării; • Descrierea contextului în care s-a desfășurat testarea; • Detalii despre rețeaua și sistemele evaluate : o echipamentele și serviciile active (adrese IP, porturi deschise,) o Tipul , versiunea, statusul actualizărilor aplicațiilor o Sistemul de operare • Prezentarea individuală a vulnerabilităților descoperite, după cum urmează: o descrierea vulnerabilității; o catalogarea vulnerabilității; o descrierea tehnică; o analiza severității și probabilității; o calcularea riscului; o 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. Ofertele trebuie să fie complete și suficient de detaliate, astfel încât să îi ofere Beneficiarului posibilitatea de a înțelege cu ușurință toate aspectele. Ofertantul va specifica versiunile și producătorii pachetelor software care se vor folosi pentru prestarea serviciilor, de asemenea se vor atașa documente de la producători în copie (file de catalog, prospecte, etc.) care să conțină caracteristicile produselor folosite. Ofertantul își va asuma răspunderea legalității utilizării instrumentelor folosite în cadrul proiectului și va trebuie sa prezinte Beneficiarului dovada utilizării legale a acestora.

Vicepreședintele grupului de lucru: **Sergiu RUSSU**

_____ **L.Ș**