Specificaţii tehnice (F4.1)

Numărul procedurii de achiziție *ocds-b3wdp1-MD-1629542927678* din *26 august 2021*

Denumirea procedurii de achiziție: ***Servicii de evaluare și de analiză a asigurării calității sistemelor Procuratura Generală***

Cod CPV	Denumirea bunurilor	Modelul articolului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7	8
72212900-8	**Servicii de evaluare și de analiză a asigurării calității sistemelor (servicii de testare a securității sistemului informatic al Procuraturii Generală, Procuraturilor specializate și teritoriale)**		MD	Logical Point	**Specificațiile tehnice obiectului 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	Garantăm respectarea condițiilor de la punctele 1.1, 1.2, 1.3, 1.4, 1.5, a Caietului de Sarcini. Serviciile Ofertantului le vom presta conform Specificației tehnice propuse de către autoritatea contractantă și anume: - Se va aplica testarea de penetrare etică a infrastructurii expuse în internet, inclusiv aplicațiile; - Se va aplica testarea de penetrare etică a infrastructurii expuse în rețeaua procuraturii, inclusiv aplicațiile; - Se va identifica și evalua vulnerabilitățile (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	

					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.	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 va implica o analiză activă a sistemelor informatice pentru vulnerabilitățile existente care ar putea rezulta din configurația inadecvată și din breșe cunoscute sau necunoscute de securitate cibernetică, hardware și software. Prin testarea securității sistemelor informatice se va identifica posibilele vulnerabilități existente la nivelul sistemelor hardware, bazelor de date și aplicațiilor software încorporate, furnizînd echipelor IT ale autorității, care asigură operarea, întreținerea și dezvoltarea acestora, informații și recomandări destinate remedierii vulnerabilităților identificate. Se va oferi recomandări de remediere a problemelor și vulnerabilităților identificate care vor relata cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/ luate/folosite pentru eliminarea sau micșorarea riscului generat de problemele și vulnerabilitățile detectate,	

					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.	precum și, recomandări și propuneri de implementare ale acestora. Toate serviciile descrise mai sus vor fi prestate de către specialiști locali cu o experiență de peste 14 ani, certificați internațional în: CEH, ECSA, LPT, ISC², CCSP, CISSP, CSSLP, PCIP ș.a.	

Semnat: **electronic** Numele, Prenumele: **Melnic Ion** În calitate de: **Administrator**

Ofertantul: **LogicalPoint SRL** Adresa: **mun. Chișinău str. A.Pușkin 5B**

Data: *19 septembrie 2021*