LOGICALPOINT

Anexa nr.22
la Documentația Standard

Specificaţii tehnice

Digitally signed by Melnic Ion
Date: 2022.11.16 10:24:57 EET
Reason: MoldSign Signature
Location: Moldova

Numărul procedurii de achiziţie nr. ocds-b3wdp1-MD-1667466615620 din 3 noiembrie 2022

Obiectul achiziţiei: **Servicii testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS pentru anul 2022, la solicitarea Benificiarului)**

Denumirea serviciilor	Denumirea modelului serviciului	Ţara de origine	Produ-cătorul	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
Servicii testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS pentru anul 2022, la solicitarea Benificiarului)						
Servicii testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS pentru anul 2022, la solicitarea Benificiarului	Servicii testare informatica pentru identificarea și evaluarea vulnerabilități lor a infrastructurii IT externe al CNAS pentru anul 2022, la solicitarea Benificiarului	R.Moldova	Logical Point	**Cerințe pentru servicii de testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS.** **1. Scopul și aria de acoperire a serviciilor de pentest:** 1.1.Testarea securității a CNAS se va realiza din extern la nivel de site oficial al organizației, sistemele informaționale publice, are ca scop obținerea unei perspective asupra daunelor potențiale și a riscului de bussines-procesele pe care vulnerabilitățile existente le-ar putea provoca. 1.2.Resursele care sunt expuse testelor de penetrare sunt: 1.2.1. 43 IP adrese externe, oficiile teritoriale. 1.2.2. 8 aplicațiilor web. 1.3. Testele de penetrare externe presupun scopul evaluarea securității a perimetrul extern (expus în Internet) al CNAS, în special pentru sistemele critice conectate la Internet sau accesibile din exteriorul infrastructuri a organizației. În cadrul acestor teste vom evalua orice tip de acces unic din exterior la infrastructura privată al CNAS, inclusiv serviciile care au acces limitat la adrese IP externe individuale. 1.4.Testele de penetrare vor include in mod minimal: a. Obținerea informațiilor din domeniul public b. Scanarea sistemelor din scop c. Tehnici de enumerare	*Specificația tehnică răspunde tuturor cerințelor cu privire la serviciile de testare informatică pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS pentru anul 2022. Metodologia de testare LogicalPoint se aliniază standardelor internaționale de domeniu și este descrisă în Oferta Tehnică LogicalPoint. (conform Anexei)*	Moldova Standard ISO 9001 ISO 27001 NIST ISC2

				- Identificarea sistemelor de operare - Identificarea patch-urilor de securitate lipsa pe un anumit sistem de operare. - Determinarea vulnerabilităților cunoscute la nivelul sistemelor de operare - Identificarea tuturor porturilor deschise - Identificarea serviciilor care rulează pe un anumit port - Determinarea vulnerabilităților cunoscute la nivelul serverelor de aplicații - Determinarea vulnerabilităților cunoscute pentru bazele de date - Determinarea vulnerabilităților cunoscute la nivelul serviciilor active identificate - Identificarea problemelor de configurare - Exploatarea vulnerabilităților identificate d. Obținerea accesului neautorizat prin exploatarea vulnerabilităților respectiv a problemelor de configurație e. Consolidarea accesului 1.5.Metodologia de testare elaborata si folosita de către ofertant va fi în conformitate cu bunele practici internaționale precum: (OWASP, OSSTMM, ISSAF, NIST, ISACA, etc). 1.6.In realizarea testelor de penetrare, ofertantul va realiza următorii pași: a. Construirea unui model al amenințărilor. Investigarea arhitecturii infrastructurii si a tehnologiei. Identificarea specificațiilor cheie de securitate și a amenințărilor. Crearea unui model al amenințărilor care documentează activele care trebuie protejate, potențialele amenințări la adresa acestor active, atacuri care ar putea fi realizate, precum si condițiile care ar duce la atacuri de succes. b. Construirea unui plan de evaluare și acțiune. Convertirea amenințărilor posibile în atacuri care vor fi realizate de ingineri de securitate. Condițiile unui atac, descrise in modelarea amenințărilor, sunt testate. c. Executarea evaluării. Executarea atacurilor, așa cum sunt descrise în planul de acțiune. Descoperirea vulnerabilităților și a variațiilor acestora. d. Raportarea rezultatelor. Documentarea problemelor identificate și prezentarea unor recomandări pentru remediere. 1.7.Cerințe fața de testele de penetrare pentru aplicațiile web. Testarea de securitate la nivelul aplicațiilor web este realizata în concordanță cu		

				metodologia OWASP, certificata la nivel mondial. Atacurile din planul de testare vizează în principal următoarele aspecte: a. Testarea mecanismelor de păstrare a confidențialității si integrității datelor b. Testarea procesului de Management al Identitarii c. Testarea mecanismelor de Management al configurațiilor d. Testarea mecanismelor de Autentificare e. Testarea mecanismelor de Autorizare f. Testarea mecanismelor de Management al Sesiunilor g. Testarea mecanismelor de Validare a Datelor h. Testarea mecanismelor de management al Excepțiilor (erorilor) i. Testarea mecanismelor Criptografice j. Testarea problemelor de Logica de Business. 1.8.Cerințe fata de descrierea vulnerabilităților identificate. Partea executiva va conține descrierea pe scurt a problemelor si vulnerabilităților identificate si va utiliza metode grafice (cel puțin diagrame, grafice sau harți). Partea tehnica va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Raportul va conține cel puțin următoarele capitole: a. Sumar executiv; b. Obiectivele și scopul evaluării; c. Prezentare succinta a metodologiei utilizate in cadrul testării; d. Descrierea contextului în care s-a desfășurat testarea; e. Prezentarea individuala a vulnerabilităților descoperite, după cum urmează: - Descrierea vulnerabilității; - Catalogarea vulnerabilității; - Descrierea tehnica; - Analiza severității si probabilității; - Calcularea riscului; - Contramăsuri recomandate pentru remediere. e. Alte detalii si recomandări; f. Anexa cu lista testelor de securitate efectuate. 1.9.Cerințe fata de analiza de risc. In vederea realizării acestei analize de risc, se realizează următoarele:		

				a. Identificarea elementelor analizate: sisteme, aplicații, procese, oameni b. Identificarea vulnerabilităților și a amenințărilor; c. Cuantificarea și măsurarea scenariilor de risc; d. Identificarea controalelor aplicabile; e. Stabilirea registrului de riscuri și identificarea riscurilor reziduale sau a scenariilor necontrolate. 1.10. Cerințe fața de raportul de prezentare și follow-up. Raportul are ca scop prezentarea concluziilor primare și a analizelor rezultate din datele culese în procesul de testare. În urma finalizării activităților de testare, în cadrul unei ședințe de închidere tip workshop, ofertantul va prezenta concluziile activității de testare și va realiza agrearea cu observațiile beneficiarul testării pe principalele domenii funcționale. De asemenea, în cadrul ședinței va fi prezentat, în forma draft, "Raportul de testare", raport care va fi îmbunătățit pe baza rezultatelor dezbaterilor. Raportul de testare va include: a. Limitări privind divulgarea și utilizarea raportului de testare a vulnerabilităților; b. Introducere (rezumat al serviciilor prestate, aria de acoperire și perioada); c. Sumar executiv: - Obiectivele și scopul testului de scanare a vulnerabilităților; - Descrierea contextului în care s-a desfășurat testul de penetrare; d. Prezentarea individuala a vulnerabilităților descoperite, după cum urmează: - Descrierea vulnerabilității; - Catalogarea vulnerabilității; - Descrierea tehnica; - Analiza severității si probabilității; - Calcularea riscului; - Contramăsuri recomandate pentru remediere. - Alte detalii si recomandări; e. Identificarea vulnerabilităților precum: - Generale; - Clasificate pe categorie; - Clasificate pe risc; - Raport al vulnerabilităților în detaliu care va conține: un sumar, scoring-ul		

				de risc, descrierea riscului, descrierea tehnică. f. Anexa cu lista testelor de securitate efectuate. 1.11. După confirmarea remedierii vulnerabilităților identificate de către beneficiar, ofertantul va realiza o retestare pentru a confirma închiderea vulnerabilităților identificate. **2. Cerințe față de membrii echipei de proiect:** 2.1. Compania care va presta serviciile de penetrare trebuie să prezinte dovezi că poate pune la dispoziție un număr minim de experți-cheie precum: **a. Manager de proiect –** responsabil de coordonarea echipei de experți și managementului proiectului în sine. 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Se va/vor prezenta CV-ul acestuia. **b. Expert Securitate sisteme informaționale –** responsabil de coordonarea echipei de experți în realizarea testelor de penetrare: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Experiența va fi dovedită prin certificat internațional acreditat în calitate de auditor intern securitate informațională ISO 27001, (CISA) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. **c. Expert testare securitate infrastructură rețea –** responsabil de testarea de penetrare a infrastructurii de rețea: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. 2. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Offensive Security Certified Professional (OSCP) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. **d. Expert testare securitate sisteme informatice –** responsabil de testarea de penetrare a aplicațiilor web: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. 2. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Licensed Penetration		

				Tester (LPT) sau echivalentul, GIAC Cloud Penetration Tester (GCPN) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. 3. Cunoștințe avansate privind sisteme de operare, baze de date, sisteme de virtualizare dovedite prin diplome sau experiența – CV. **3. Alte cerințe minim obligatorii față de ofertant:** 3.1. Compania ce va presta serviciile de penetrare trebuie să posede o experiență specifică în prestarea serviciilor similar de cel puțin 3 ani în domeniu și minim 3 recomandări (sau 3 contractare similare) pe piața locala din R. Moldova în ultimii 3 ani. 3.2. Compania ce va presta serviciile de penetrare trebuie să dețină competență în domeniul de activitate în servicii privind asigurarea securității informației, teste de penetrare și auditarea sistemelor informatice. 3.3. Semnarea acordului de confidențialitate ((NDA) Non-Disclosure Agreement) cu compania și echipa de implementarea serviciilor.		
TOTAL						

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

Ofertantul: LogicalPoint SRL Adresa: mun.Chisinau str. A.Puskin 5B