UNIUNEA EUROPEANĂ

Fondul Social European

GUVERNUL ROMANIEI

Ministerul Dezvoltării Regionale și Administrației Publice

Inovaţie în administraţie

Programul Operaţional "Dezvoltarea Capacităţii Administrative"

Caiet De Sarcini

Sistemul National de Combatere a Criminalitatii Informatice „Cyber Crime”

CENTRUL NAŢIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ (CERT-RO)

Caietul de sarcini este elaborat în concordanţă cu necesităţile obiective ale Autoritatii Contractante, face parte integrantă din Documentaţia pentru ofertanti pentru atribuirea contractului de servicii de consultanta pentru crearea unui cadru de lucru adecvat in vederea cresterii capacitatii de formulare a politicilor publice si de realizare a unei mai bune reglementari si planificari strategice prin consolidarea parteneriatelor atat la nivel inter-institutional cat si intre institutiile publice si reprezentantii altor domenii interesati in combaterea criminalitatii informatice.

Caietul de sarcini conţine, în mod obligatoriu cerinţele tehnice impuse ce vor fi considerate ca fiind minimale.

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 cerinţelor minimale din Caietul de sarcini. Ofertele de servicii care nu satisfac cerinţele caietului de sarcini vor fi declarate oferte neconforme şi vor fi respinse.

Cuprins

ABREVIERI ŞI ACRONIME

UE	Uniunea Europeană
CERT-RO	Centrul National de Raspuns la Incidente de Securitate Cibernetica
MSI	Ministerul pentru Societatea Informationala
MAI	Ministerul Afacerilor Interne
CSAT	Consiliul Suprem de Aparare a Tarii
CEE/ONU	Comisia Economică pentru Europa a Organizației Națiunilor Unite
CNMSI	Centrul National de Management al Societatii Informationale
ICI	Institutul Naţional de Cercetare-Dezvoltare în Informatică
IGPR	Inspectoratul General al Politiei Romane
PICCJ	Parchetul de pe langa Inalta Curte de Casatie si Justitie
INM	Institutul National de Magistratura
OIPC-INTERPOL	Organizatia Internationala de Politie Criminala
EUROJUST	Agentia Uniunii Europene de cooperare judiciara
ONU	Organizatia Natiunilor Unite
ENISA	Agenția Europeană pentru Securitatea Rețelelor și a Informației

1 Informaţii generale

1.1 Informaţii privind autoritatea contractantă

Centrul National de Raspuns la Incidente de Securitate Cibernetica – CERT-RO a fost infiintat prin Hotararea de Guvern nr. 494/2011, ca organ de specialitate al administratiei publice centrale, cu personalitate juridica, in coordonarea Ministerului pentru Societatea Informationala, finantat integral de la bugetul de stat.

CERT-RO isi desfasoara activitatea in conformitate cu legislatia in vigoare si cu regulamentul propriu de organizare si functionare, in scopul realizarii **prevenirii, analizei, identificarii si reactiei la incidente in cadrul infrastructurilor cibernetice** ce asigura functionalitati de utilitate publica ori asigura servicii ale societatii informationale.

Centrul National de Raspuns la Incidente de Securitate Cibernetica - CERT-RO asigura servicii publice de tip preventiv si reactiv, precum si servicii publice de consultanta pentru managementul calitatii serviciilor de securitate cibernetica:

- anunturi privind evenimente in domeniu;
- anunturi privind amenintari nou identificate pe plan national si international;
- cercetare si informare privind noutatile tehnologice in domeniu;
- realizarea, la cerere, de auditari si evaluari de securitate sau teste de penetrare;
- estimarea vulnerabilitatilor si punerea la dispozitie de situatii actualizate privind incercarile de intruziune si servicii de localizare a surselor atacurilor, pe baza informatiilor transmise de furnizorii de retele si servicii de comunicatii electronice;
- diseminarea informatiilor de securitate cibernetica.
- alerte si atentionari privind aparitia unor activitati premergatoare atacurilor;
- gestiunea incidentelor la nivel national, in cooperare cu celelalte echipe CERT;
- diseminarea rezultatelor investigatiilor incidentelor de securitate cibernetica, cu respectarea prevederilor acordurilor de cooperare incheiate cu partenerii CERT-RO;
- analize de risc aplicate la nivel local si la nivel national privind infrastructurile cibernetice;
- planificarea asigurarii functionarii continue si a recuperarii in caz de dezastre;
- atestarea managementului securitatii cibernetice si a incidentelor cibernetice;
- pregatirea echipelor de tip CERT, a echipelor de audit in domeniul securitatii retelelor, cu prioritate a celor incluse in infrastructura critica nationala.

CERT-RO are urmatoarele atributii:

a) ofera servicii publice de tip preventiv, de tip reactiv si de consultanta;

b) organizeaza si intretine un sistem de baze de date privind amenintarile, vulnerabilitatile si incidentele de securitate cibernetica identificate sau raportate, tehnici si tehnologii folosite pentru atacuri, precum si bune practici pentru protectia infrastructurilor cibernetice;

c) asigura cadrul organizatoric si suportul tehnic necesar schimbului de informatii dintre diverse echipe de tip CERT, utilizatori, autoritati, producatori de echipamente si solutii de securitate cibernetica, precum si furnizori de servicii in domeniu;

d) organizeaza, desfasoara sau participa la activitati de instruire in domeniul securitatii cibernetice;

e) organizeaza simpozioane, dezbateri pe teme de securitate cibernetica si asigura diseminarea unor informatii specifice prin mass-media;

f) desfasoara activitati de cercetare-dezvoltare in domeniu si elaboreaza proceduri si recomandari privind securitatea cibernetica, potrivit prevederilor legale privind cercetarea stiintifica si dezvoltarea tehnologica;

g) asigura MSI suportul tehnic si de specialitate pentru elaborarea politicilor de securitate cibernetica necesar a fi respectate de furnizorii de retele si servicii de comunicatii electronice publice pentru obtinerea autorizarii de functionare a acestora, precum si la evaluarea modului de implementare a acestora;

h) asigura consultanta de specialitate autoritatilor publice responsabile, stabilite conform Ordonantei de urgenta a Guvernului nr. 98/2010 privind identificarea, desemnarea si protectia infrastructurilor critice, aprobata cu modificari prin Legea nr.18/2011, cu privire la produsele si sistemele de securitate cibernetica care deservesc infrastructurile critice nationale si europene;

i) asigura puncte de contact pentru colectarea sesizarilor si a informatiilor despre incidente de securitate cibernetica atat automatizat, cat si prin comunicare directa securizata, dupa caz;

j) identifica, analizeaza si clasifica incidentele de securitate din cadrul infrastructurilor cibernetice, conform ariei de competenta;

k) elaboreaza propuneri pe care le inainteaza catre MSI sau CSAT, privind modificarea cadrului legislativ in vederea stimularii dezvoltarii securitatii infrastructurilor cibernetice ce asigura functionalitati de utilitate publica ori asigura servicii ale societatii informationale;

l) planifica si programeaza in proiectul de buget propriu resursele financiare necesare in vederea realizarii politicilor in domeniile sale de competenta;

m) coordoneaza derularea proiectelor, ale caror beneficiari sunt MSI si/sau institutiile din subordinea acestuia, cu finantare nationala sau internationala in domeniul securitatii infrastructurilor cibernetice ce asigura functionalitati de utilitate publica, ori asigura servicii ale societatii informationale, care vizeaza capacitatea institutionala operationala a CERT-RO;

n) asigura MSI suportul tehnic si de specialitate pentru urmarirea si controlul aplicarii prevederilor cuprinse in actele normative in vigoare sau in acordurile internationale in domeniul de competenta si notifica organele competente pentru demararea procedurilor legale in vederea cercetarii si sanctionarii, dupa caz.

1.2 Descrierea cadrului existent

Domeniul criminalitatii cibernetice a capatat in ultima perioada o dimensiune care nu mai poate fi ignorata, fiind nevoie stringenta de o strategie nationala in domeniul securitatii informatiei.

Într-o societate in care zilnic se face uz de calculatoare în aproape toate domeniile, de la controlul traficului aerian, feroviar şi transportul in comun şi până la coordonarea serviciilor medicale şi securitatea naţională, o dificultate aparent neinsemnata în funcţionarea acestor sisteme poate pune în pericol mii de vieţi omeneşti. Acest fapt ne demonstrează incidenţa noilor tehnologii asupra fiinţei umane, pe de o parte, şi, pe de altă parte, dependenţa societăţii faţă de noile sisteme informatizate.

Criminalitatea cibernetică poate să aibă un preţ foarte ridicat pe plan economic, dar şi în termenii securităţii societatii. Problema definirii delictului informatic poate apărea ca o preocupare de noutate pentru societăţile unde accesul noilor tehnologii s-a făcut cu întârziere şi unde statul nu a luat încă toate măsurile de protecţie împotriva crimelor care pot fi comise cu ajutorul acestora.

Protejarea retelelor de calculatoare este considerata drept o prioritate pentru reprezentantii guvernului in toate statele membre, in special datorita nevoii de protejare a datelor, de asigurare a unei economii functionale, din motive de asigurare a securitatii nationale si de promovare a comertului electronic.

Acest interes a condus la un ansamblu substantial de precautii legale in cadrul Directivelor UE in ceea ce priveste protectia datelor si a Cadrului UE pentru telecomunicatii. Aceste masuri insa trebuie aplicate intr-un mediu dinamic din punct de vedere al schimbarilor si al aparitiei de noi tehnologii, pietei concurentiale, convergentei retelelor si globalizarii, provocari ce nu se coreleaza cu tendinta pietei de a nu investi suficient in componenta de securitate.

Atat in cadrul „Conventiei Consiliului Europei privind Criminalitatea Informatică”, adoptată la Budapesta la 23 noiembrie 2001 cat si in Conferinţa Internaţionala „Cooperarea împotriva Criminalităţii Informatice”, Consiliul Europei, Strasbourg, 1-2 aprilie 2008, se incurajeaza crearea unei baze juridice solide pentru cooperarea între sectoarele public şi privat, organele de cercetare, precum şi pentru cooperarea internaţională.

Exista atat la nivel al UE cat si la nivel global o tendinta de armonizare legislativa in privinta criminalitatii informatice. Un aspect deosebit de relevant il contituie globalizarea infractiunilor informatice, orice proiect national in acest domeniu trebuind sa includa si abordarea internationala a situatiei. Conform datelor oficiale, in anul 2010 peste 1/3 din populatia lumii este conectata la internet, accesul liber si neingradit facilitand insa si infractionalitatea cibernetica.

In ciuda masurilor adoptate, situatia pe plan mondial in domeniul securitatii informatice se caracterizeaza printr-o tendinta de crestere continua a criminalitatii, România fiind perceputa ca un factor exportator de instabilitate in domeniu.

Pozitia Romaniei in statisticile ultimilor ani privind criminalitatea informatica este ingrijoratoare. Conform unui raport din 2009, Romania se afla pe locul 10 ca si principala locatie de gazduire malware (Sursa Cyveilance 2009) si pe locul 7 ca tari “gazda” in cazul atacurilor de tip pishing (Sursa Cyveilance 2009).

Conform raportului MAI pe 2009 privind Criminalitatea Informatica, tehnologia IT&C este folosita tot mai intens in comiterea de infractiuni in general. În primele sapte luni ale anului, au fost identificate 77 de grupări infracţionale, compuse din 447 membri care îşi desfăşoară activitatea pe linia criminalităţii informatice şi au fost destrămate 21 grupări infracţionale, compuse din 248 membri. De asemenea, au fost finalizate cercetările în 56 de cazuri, fiind soluţionate 364 de infracţiuni, privitor la 269 de persoane care au fost trimise în judecată, 167 dintre acestea fiind reţinute sau arestate. Imaginea creionata de acest raport este sumbra si ridica un important semnal de alarma privind proliferarea criminalitatii informatice.

Din aceste considerente, la nivel national se impune o abordare moderna, integratoare, in domeniul securitatii, concretizata printr-un set de politici publice si acte normative la elaborarea si aplicarea carora trebuie sa participe toate entitatile abilitate, constietizand astfel necesitatea unei colaborari reale in folosul institutiilor publice cu impact direct asupra utilizatorilor de servicii electronice, fie ei cetateni sau reprezentanti ai mediului de afaceri.

Pentru a veni in sprijinul initiativelor MSI in domeniu consideram mai mult decat oportuna extinderea capabilitatilor CERT-RO care sa puna bazele unei colaborari reale intre institutiile statului roman abilitate sa monitorizeze mediul virtual si sa intervina in cazul unor atacuri informatice, valorificand rezultatele acestei implicari prin transpunerea lor intr-un set de politici publice utile, coerente si moderne, aplicabile de catre toti participantii la mediul on-line.

In acest context, incepand cu luna aprilie 2012, CERT-RO, este responsabila, in calitate de beneficiar de implementarea proiectului intitulat “Sistemul National de Combatere a Criminalitatii Informatice Cyber Crime” (cod SMIS 37595), finantat din Fondul Social European prin Programul Operational Dezvoltarea Capacitatii Administrative, Axa prioritara 1 – imbunatatiri de structura si proces a

managementului ciclului de politici publice, Domeniul major de interventie 1.1 – Imbunatatirea procesului de luare a deciziilor la nivel politico-administrativ.

2 Scopul proiectului şi rezultatele aşteptate

2.1 Obiectivul general al proiectului

Obiectivul general al proiectului intitulat “Sistemul National de Combatere a Criminalitatii Informatice Cyber Crime” (cod SMIS 37595) si finantat prin PODCA este acela de a crea un cadru de lucru adecvat in vederea cresterii capacitatii de formulare a politicilor publice si de realizare a unei mai bune reglementari si planificari strategice prin consolidarea parteneriatelor atat la nivel inter-institutional cat si intre institutiile publice si reprezentantii altor domenii interesati in combaterea criminalitatii informatice.

Scopul proiectului este reprezentat de:

- elaborarea unui **raport** pentru stabilirea principalilor indicatori de performanta utilizati in **evaluarea gradului de criminalitate informatica la nivel national** si analiza lor la momentul inceperii proiectului in comparatie cu nivelul de referinta al Unuiunii Europene;
- constituirea a **doua grupuri de experti calificati** in principalele domenii de specialitate (tehnic si legislativ) ce vor constitui baza de lucru si suport pentru indeplinirea obiectivului strategic al proiectului;
- **diseminarea si optimizarea rezultatelor** activitatii desfasurate de grupurile de experti in cadrul a **cinci evenimente de tip “ateliere de lucru”** intre reprezentanti ai companiilor de IT&C / administratiei publice / mediul educational, experti din cadrul proiectului si experti externi;
- prezentarea obiectivelor proiectului, cu accent pe **importanta colaborarii inter-institutionale**, si a rezultatelor obtinute in cadrul a **trei evenimente de tip conferinta** cu reprezentanti din toate sectoarele interesate din Romania si din alte state membre;
- **cresterea nivelului de pregatire si calificare a personalului** specializat prin organizarea unui numar de **patru cursuri de specialitate** pentru 40 de reprezentanti desemnati din cadrul institutiilor abilitate sa colaboreze in combaterea criminalitatii informatice in Romania;
- **cooptarea si constientizarea personalul de decizie** din cadrul institutiilor abilitate sa conlucreze in domeniul proiectului prin organizarea unui numar de **cinci intalniri** in vederea dezbaterii rezultatelor activitatii celor doua grupuri (tehnic si legislativ), a problemelor survenite si propunerilor elaborate;
- **cristalizarea si uniformizarea conceptelor specifice domeniului si diseminarea acestora in randul celor interesati prin intermediul materialelor de promovare si a unui portal web dedicat.**

2.2 Obiective specifice

Obiectivele specifice ale prezentului contract constau în:

- stabilirea principalilor indicatori de performanta utilizati in evaluarea gradului de criminalitate informatica la nivel national si analiza lor la momentul inceperii proiectului in comparatie cu nivelul de referinta al Unuiunii Europene;
- implementarea unei platforme tehnologice specializate si la standarde actuale pentru pregatirea continua a specialistilor din administratia publica in aspecte privind securitatea informatica;
- corelarea si actualizarea reglementarilor si actelor normative din domeniu prin definirea unui set de politici publice, acte normative și proceduri în vederea combaterii criminalității informatice;
- instruirea și certificarea membrilor echipei ”Cyber Crime”, pentru a se pune la curent cu ultimele cunoștinte în materie soluții de contracarare a criminalității informatice.

2.3 Rezultatele aşteptate

Prin prezentul proiect, autoritatea contractanta isi propune sa contribuie la rezolvarea problemelor din domeniul criminalitatii informatice prin corelarea si actualizarea reglementarilor si actelor normative din domeniu, realizarea unui cadru de securitate a mediului virtual bazat pe politici publice eficiente. Se are in vedere atat aspectul de preventie si educare cat si realizarea de modele standardizate de evaluare si interventie in caz de atac informatic, proceduri de lucru eficiente si usor de implementat intr-un cadru de lucru multi-organizational, in stransa colaborare cu organismele similare din alte state membre si corelate totodata cu tendintele si directivele europene in domeniu.

Rezultatele așteptate în urma implementării prezentului contract:

- Raport privind indicatorii de performanta utilizati in evaluarea gradului de criminalitate informatica la nivel mondial si propunerile de optimizare a situatiei acestui tip de indicatori la nivel national;
- Platformă tehnologică implementată și funcțională la standarde actuale pentru pregatirea continuă a specialiștilor din administrația publică în aspecte privind securitatea informatică;
- Set de politici publice, acte normative și proceduri elaborate, în vederea combaterii criminalității informatice;
- 40 persoane – membri ai echipei Cyber Crime – instruiți și certificați în domeniul soluțiilor de contracarare a criminalității informatice.

3 Premise şi riscuri

3.1 Premise privind implementarea proiectului

1. Nu vor avea loc schimbari institutionale/legale majore care sa afecteze scopul si obiectivele proiectului;
2. Autoritatea contractanta (CERT-RO) va asigura sprijin pentru facilitarea accesului Prestatorului la reuniunile/intalnirile de lucru interinstitutionale ce vor fi organizate si pentru asigurarea contactelor cu institutiile si persoanele relevante, precum si accesul la diversele surse de informare.

3.2 Riscuri

Riscuri posibile :

- Risc de implementare – este posibil ca institutiile administratiei publice centrale direct interesate de combaterea criminalitatii informatice sa nu puna la dispozitie experti in vederea participarii la implementarea proiectului;
- Risc institutional-legislativ – in cadrul intrunirilor la nivel decizional este posibil ca factorii de decizie din institutiile participante sa nu actioneze cu promptitudine in vederea initierii unor acte normative care sa sustina combaterea criminalitatii informatice;
- Risc aferent furnizorilor – ciclul de viata al companiilor poate fi scurtat datorita recesiunii economice /progresul tehnologic poate duce la scoaterea companiilor de pe piata;
- Risc tehnologic – tehnologia informatiei este caracterizata de un dinamism greu de egalat. Noi standarde si protocoale IT sunt dezvoltate in permanenta, iar imaginea internetului se schimba in mod constant.

4 Scopul prestațiilor

4.1 Descrierea proiectului

Prin implementarea proiectului se doreste constientizarea si responsabilizarea actorilor direct implicati (furnizori de servicii IT&C, producatori si comercianti de solutii de securitate, echipamente IT&C si software, autoritati cu responsabilitati in domeniu) si **crearea unei educatii privind securitatea in mediul virtual la nivelul intregii societati.**

Contractul care face obiectul prezentei proceduri presupune urmatoarele activitati:

1. Consultanta pentru definirea indicatorilor de criminaliate informatica si analiza situatiei actuale (*activitatea 5 a proiectului*)

2. Implementarea soluției informatice si furnizarea echipamentelor aferente (*activitatea 6 a proiectului)*
3. Definirea unui set de politici publice, acte normative si proceduri in vederea combaterii criminalitatii informatice (*activitatea 7 a proiectului*)
4. Instruirea si certificarea membrilor echipei „Cyber Crime" si secretariatului permanent (sub-*activitatea 8.4 a proiectului*)

4.2 Zona geografică ce se urmarește a fi cuprinsă

Aria de acoperire geografica a proiectului este Romania. Proiectul va fi organizat in București.

4.3 Grupurile ţintă

Grupul tinta este un grup interministerial format din reprezentanti ai institutiilor beneficiare vizate, ce vor fi implicati in diferitele activitati ale proiectului.

Beneficiarul proiectului este Centrul National de Răspuns la Incidente de Securitate Cibernetică CERT-RO infiintat prin Hotararea de Guvern nr. 494/2011, ca organ de specialitate al administratiei publice centrale, cu personalitate juridica, in coordonarea Ministerului Comunicatiilor si Societatii Informationale.

Beneficiarii indirecti ai proiectului sunt:

- Ministerul Justitiei
- Ministerul Afacerilor Interne;
- Serviciul Roman de Informatii - SRI;
- Serviciul de Informatii Externe - SIE;
- Ministerul Apararii Nationale;
- Administratia Prezidentiala;
- Secretariatul General al Guvernului;
- Ministerul pentru Societatatea Informationala;
- Institutul de Cercetare – Dezvoltare in Informatica;
- Centrul National de Management pentu Societatea Informationala;
- Autoritatea Nationala pentru Reglementare in Comunicatii si Tehnologia Informatiei
- Oficiul Registrului National al Informatiilor Secrete de Stat
- Serviciul de Telecomunicatii Speciale
- structuri de securitate din toate tipurile de organizatii;
- echipe IT cu sarcini de linie pe securitate IT&C;
- provideri de servicii IT&C;
- producatori, comercianti si integratori de solutii de securitate;
- producatori de echipamente IT&C si de software;

- comercianti de echipamente IT&C si de software;
- utilizatori ai serviciilor electronice din Romania si toate statele membre.

4.4 Calendarul de implementare

In implementarea contractului, Prestatorul este obligat sa respecte calendarul de implementare a activitatilor proiectului, in conformitate cu cererea de finantare, dupa cum urmeaza (**L13 se considera luna semnarii contractului**):

Nr.	Activitate	Descrierea activităţii	Durata	Cost lei (fără TVA)
5.	**Consultanta pentru definirea indicatorilor de criminaliate informatica si analiza situatiei actuale**	**In cadrul acestei activitati se va elabora un studiu pentru stabilirea principalilor indicatori de performanta utilizati in evaluarea gradului de criminalitate informatica la nivel national si a stadiului lor la momentul inceperii proiectului in comparatie cu nivelul de referinta al Unuiunii Europene. Studiul se va finaliza cu un raport care sa contina informatiile colectate si un set de masuri si propuneri concrete pentru optimizarea situatiei existente**	**L13 – L15**	**1.375.000,00**
5.1	Definirea principalilor indicatori de performanta utilizati in evaluarea gradului de criminalitate informatica	Se stabileste setul de indicatori in baza carora se vor face analizele de performanta in domeniul criminalitatii informatice, tinind cont de indicatorii utilizati la nivel mondial.	L13-L14	412.500,00
5.2	Analizarea gradului de realizare a indicatorilor stabiliti la momentul inceperii derularii proiectului	Se va analiza gradul de satisfactie a indicatorilor stabiliti a fi luati in calcul in cadrul analizei comparativ cu alte tari pentru a avea o imagine foarte clara a pozitiei Romaniei in clasamentele de criminalitate informatica (locatii de gazduire malware, tari „gazda” pentru atacuri de phishing, si alte domenii unde tara noastra ocupa o pozitie considerabila in criminalitate informatica)	L14-L15	412.500,00
5.3	Elaborare raport privind masurile si propunerile de optimizare a situatiei	In urma analizei cu privire la pozitia tarii noastre privind criminalitatea informatica, consultantul va elabora o analiza detaliata a situatiei actuale si mai ales a masurilor ce se impun in remedierea situatiei existente intr-un raport de optimizare.	L15	550.000,00

6	**Dezvoltarea si implementarea soluției informatice si echipamentelor aferente**	**Dezvoltarea sistemului informatic compus din aplicatii necesare simularii diverselor tipuri de atacuri informatice si formularii tipurilor de masuri de prevenire si de raspuns**	**L13-L17***	**1.100.000,00**
6.1.	Analiză tehnică soluţie pe baza specificaţiilor rezultate în urma fazei de analiză detaliată	Analiza cerintelor si functionalitatilor pe care trebuie sa le indeplineasca sistemul informatic implementat si transpunerea cerintelor functionale depistate in etapa de consultanta, in cerinte software	L13-L14	184.000,00
6.2.	Livrare echipamente hardware	Echipamente livrate pentru servere şi staţii de lucru	L13-L14	475.000,00
6.3.	Instalare echipamente hardware	Echipamente instalate pentru servere şi staţii	L14	21.000,00
6.4.	Proiectare şi programare soluţie	Dezvoltarea si implementarea solutiei informatice si a portalului web; crearea de scenarii de lucru pentru echipa Cyber Crime	L14-L16	336.000,00
6.5.	Integrarea modulelor a portalului web si testarea soluţiei software dezvoltate	Integrarea modulelor si portalului web si testarea soluţiei software dezvoltate	L16-L17	63.000,00
6.6	Instruire administratori de sistem	Vor fi instruiti 3 administratori și 6 utilizatori (9 persoane) din cadrul CERT-RO pentru soluțiile implementate.	L17	21.000,00
7.	**Definirea unui set de politici publice, propuneri de acte normative si proceduri in vederea combaterii criminalitatii informatice**	**Va fi definit un set de politici publice, propuneri de acte normative si proceduri, aplicabile participantilor la traficul on-line**	**L14 – L23**	**3.630.000,00**
7.1	Activitati de analiza, documentare, suport, in vederea formularii propunerilor de strategii, proceduri si	Activitatea va fi organizata de Contractor si va fi supervizata de CERT-RO 16 experti tehnici din cadrul proiectului care vor fi responsabili cu	L14 - L21	2.178.000,00

	acte normative	activitatile de analiza, documentare, dar si cu furnizarea de cunostinte tehnice membrilor celorlalte echipe implicate in implementarea proiectului; 4 experti in legislatie si politici publice vor forma echipa legislativa din cadrul proiectului care va trebui sa furnizeze informatii cu privire la aspectele legislative nationale si internationale in vigoare; experti in legislatie si politici publice de profil din cadrul CERT-RO, MSI, CNMSI si ICI vor fi invitati sa se alature dezbaterilor si vor participa la activitatile de formulare a politicilor publice, strategiilor si actelor normative necesare		
7.2	Elaborarea documentelor de politici publice rezultate in urma studiilor,analizelor si dezbaterilor	Vor fi elaborate strategii, acte normative si proceduri coerente si moderne, usor aplicabile de catre toti participantii la traficul on-line sub forma unor actiuni concrete atat in plan legislativ cat si tehnic	L15-L23	1.452.000,00
8.4	Instruirea si certificarea membrilor echipei „Cyber Crime” si secretariatului permanent	Se vor stabili cursurile la care vor participa membrii echipei „Cyber Crime” si secretariatului permanent, sustinute in afara tarii in vederea certificarii pentru a se pune la curent cu ultimele cunostinte in materie solutii de contracarare a criminalitatii informatice.	L16-L23	1.320.000,00

4.5 Activităţi şi rezultate specifice

4.5.1 Consultanţă pentru definirea indicatorilor de criminaliate informatică şi analiza situatiei actuale (Activitatea 5 a proiectului)

Activitatea de definire a indicatorilor de criminalitate informatica presupune un proces complex de natura documentara si analiza statistica datorita necesitatii culegerii datelor statistice pe baza carora sa fie asigurata baza de identificare si definire a indicatorilor. Dificultatile intampinate in activitatea de culegere a datelor statistice se regasesc in multitudinea de diferite definitii si sisteme de clasificare a infractiunilor de natura informatica, ceea ce face ca gasirea unui numitor comun dupa care sa fie identificate si clasificate anumite tipuri de infractiuni sa implice o analiza laborioasa si implicit un volum mare de lucru. Unele pot fi lasate in afara colectarii de date statistice, altele pot fi calificate ca fiind infractiuni de natura criminalitatii informatice, iar o astfel de numaratoare fara un numitor comun poate genera date confuze, neunitare si fara consistenta. Astfel, Prestatorul va avea sarcina de a identifica, defini, si masura acesti indicatori pe baza datelor cele mai relevante, astfel incat rezultatul cercetarii sa aiba o rata de aplicabilitate si utilitate cat mai mare pentru beneficiarii finali, utilizatorii sistemelor si retelelor informatice.

In cadrul acestei activitati se va elabora un studiu pentru stabilirea principalilor indicatori de performanta utilizati in evaluarea gradului de criminalitate informatica la nivel national si a stadiului lor la momentul inceperii proiectului in comparatie cu nivelul de referinta al Uniunii Europene in context global. Documentarea pentru realizarea studiului se va realiza cel putin prin metodele de observatie, statistica si istorico-comparativa.Ca strategie de prelucrare a datelor se vor efectua analize preliminare de statistica, logica si interpretarea.Perioada de referinta ce va face obiectul studiului va fi 2010, 2011 si 2012 in masura in care sunt disponibile. Colectarea datelor principale pentru perioada de referinta va trebui sa fie efectuata de la cel putin trei concerne private recunoscute pe plan mondial in domeniul IT, organismele de specialitate de la ONU, OIPC-INTERPOL, ENISA, EUROJUST si EUROPOL. Studiul va contine un set de masuri si propuneri concrete pentru optimizarea situatiei existente, inclusiv din punct de vedere al aspectelor de ordin legislativ.

4.5.1.1 Definirea principalilor indicatori de performanta utilizati in evaluarea gradului de criminalitate informatica (Sub-activitatea 5.1)

Introducere

Prin intermediul acestor activitati, se doreste definirea principalilor indicatori de performanta utilizati in evaluarea gradului de criminalitate informatica pe baza informatiilor de natura statistica colectate de la principalele entitati implicate in asigurarea protectiei utilizatorilor in fata activitatii de criminalitate informatica.

Cerinte generale

Prestatorul va identifica setul de indicatori in baza carora se vor face analizele de performanta in domeniul criminalitatii informatice, tinand cont de datele de natura statistica culese la nivel national de la institutiile cu atributii in domeniu, de indicatiile cuprinse in documentele produse de grupul operativ CEE-ONU, de documentatia existenta la nivelul Uniunii Europene, de indicatorii utilizati la nivel mondial, de tendintele in domeniul criminalitatii informatice etc.

Cerinte specifice

Prestatorul va realiza o analiza documentara amanuntita a surselor de date existente la nivel national astfel incat sa identifice sursa cea mai relevanta:

Pentru realizarea acestei activitati, prestatorul va avea in vedere cel putin urmatorii detinatori de informatii:

- Institutul National de Statistica, precum si institutiile care functioneaza in subordonarea sa
- Ministerul Afacerilor Interne, precum si institutiile care functioneaza in subordinea, autoritatea si coordonarea sa
- MSI precum si institutiile care functioneaza in subordinea, autoritatea si coordonarea sa

Prestatorul va analiza si va prezenta in cadrul acestei activitati urmatoarele:

- Detinatorul fiecarui tip de indicator identificat
- Regularitatea culegerii datelor
- Formatul in care datele sunt detinute
- Seriile de date detinute (din ce an exista informatii colectate)
- Mijloacele tehnice prin care se vor colecta datele de la fiecare dintre sursele de mai sus
- Disponibilitatea, conditiile si modalitatile prin care autoritatile locale/nationale pot furniza datele
- Masuri de imbunatatire a colaborarilor cu autoritatile locale/nationale pentru furnizarea de date
- Impedimentele care afecteaza colectarea datelor intr-un format rezonabil
- Alti factori care pot afecta fezabilitatea colectarii datelor

Ca urmare a acestei analize, ofertantul va realiza pentru fiecare indicator identificat o fisa ce va cuprinde: **denumire, definitie, institutie oficiala producatoare de date, serii de date (periodicitate si nivel culegere).**

Indicatorii de performanta vor fi alesi pe baza urmatoarelor studii comparative:

- Standardul de practică națională in domeniul indicatorilor de performanta pentru prevenirea criminalitatii informatice;
- Standardul de practica Europeana in domeniul indicatorilor de performanta pentru prevenirea criminalitatii cibernetice;
- Standardele de practica mondiala din industriile evoluate in domeniul prevenirii criminalitatii cibernetice;
- Noile metode si practici ale producatorilor de tehnologie din industria prevenirii criminalitatii cibernetice.

Pentru a putea fi validati de catre autoritatea contractanta, si pentru a-si gasi utilitatea in practica, setul de indicatori propus va trebui sa fie definit prin minim elementele specifice mentionate mai jos:

- Nominalizarea surselor de date pentru calcularea fiecarui indicator;
- Nominalizarea cadrului institutional sau de colaborare pentru a culege datele sursa pentru fiecare indicator;
- Definitia clara si concisa a surselor de date, pentru a nu aparea confuzii sau date ne-comparabile in sursele de date diferite – pentru a reduce fenomenul de definitii diferite;
- Metoda de calcul stabilita pentru fiecare indicator;
- Gradul de incredere al indicatorilor care nu sunt calculati exhaustiv ci sunt calculati pe baza de esantionare statistica;
- Periodicitatea relevanta de calcul pentru fiecare indicator;
- Tipul de indicator;
- Grupul tinta pentru fiecare indicator;

Indicatorii ce vor rezulta in cadrul acestei etape vor trebui sa fie perfect corelati si comparabili ca metoda de calcul si relevanta cu indicatorii corespondenti de la nivelul directivelor, reglementarilor si recomandarilor Uniunii Europeane.

Livrabile

- Setul de indicatori de criminalitate informatica.

Numarul de indicatori definiti utilizati in evaluarea gradului de criminalitate informatica, se vor defini in functie de dimensiunea, modul de calcul, completitudinea si aplicabilitatea

indicatorilor selectati. Indicatorii vor trebui sa cuprinda intreg spectrul de analiza si evaluare a activitatii de criminalitate informatica, indiferent de numarul de indicatori definiti.

- Propuneri de modalitati de incorporare a acestora in acte normative in vigoare si/sau propuse.

Volumul de lucu: Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **300 de zile** de lucru.

4.5.1.2 Analizarea gradului de realizare a indicatorilor stabiliti la momentul inceperii derularii proiectului (Sub-activitatea 5.2)

Cerinte generale

Plecand de la sursele identificate în cadrul sub-activității 5.1 a proiectului, Prestatorul poate incheia protocoale de colaborare in vederea furnizarii de date, cu detinatorii acestora, pentru a facilita culegerea de date.

Prestatorul va analiza gradul de realizare a indicatorilor stabiliti a fi luati in calcul in cadrul analizei comparative cu alte tari pentru a avea o imagine foarte clara a pozitiei Romaniei in clasamentele de criminalitate informatica (locatii de gazduire malware, tari „gazda” pentru atacuri de phishing, si alte domenii unde tara noastra ocupa o pozitie considerabila in activitatile de criminalitate informatica).

Prestatorul va calcula nivelul indicatorilor stabiliti la etapa anterioara a activitatii de consultanta, astfel incat acesta sa serveasca drept nivelul T0 pentru autoritatile preocupate prin atributiilor lor de evolutia si tendintele de crestere/scadere a indicatorilor pe o perioada de timp data. Rezultatul studiului va putea fi diseminat institutiilor si autoritatilor cu atributii si responsabilitati in domeniul combaterii criminalitatii cibernetice a datelor relevante cu privire la impactul diverselor masuri de tip legislativ, operational sau strategic luate, prin intermediul calcularii unor curbe de evolutie a respectivilor indicatori.

Cerinte specifice

In cadrul acestei activitati se vor calcula indicatorii stabiliti, la intervalul de relevanta definit pentru fiecare indicator, in parte, in cadrul proiectului. Se va incerca acoperirea unei arii cat mai largi de analiza, luand in calcul urmatoarele criterii de derulare a analizei:

Criteriul completitudinii – Durata de timp pe care se va rula calculul de indicatori va trebui sa permita calculul unui numar suficient de instante ale fiecarui indicator, astfel incat rezultatele obtinute sa aiba relevanta din punct de vedere al unor serii statistice.

Criteriul reprezentativitatii statistice:

- reprezentativitate geografica – se vor analiza date din diferite surse geografice;
- reprezentativitate temporala – se vor analiza date din diverse intervale de timp: ora din zi, zi din saptamana, luna;

Criteriul reproductibilitatii care impune precizarea metodologiei de culegere de date, a parametrilor instrumentarului folosit, a etapelor de prelucrare primara a inregistrarilor, a algoritmilor folositi in prelucrare, precum si precizarea oricaror alte informatii necesare pentru reproducerea ulterioara a analizei.

In cadrul acestei activitati prestatorul va realiza un studiu comparativ intre rezultatele obtinute in cadrul analizei de indicatori la nivelul Romaniei, cu rezultatele indicatorilor corespondenti, obtinute la nivelul altor organizatii similare din Uniunea Europeana, in masura in care acestea sunt disponibile, astfel incat sa rezulte o analiza completa a situatiei nationale in contextul European.

Livrabile

- Seturile de date obtinute in urma analizei gradului de indeplinire a indicatorilor de criminalitate cibernetica
- Studiu comparativ intre nivelul indicatorilor la nivel national versus nivelul UE.

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **300 de zile** de lucru.

4.5.1.3 Elaborare raport privind masurile si propunerile de optimizare a situatiei (Sub-activitatea 5.3)

Cerinte generale

In urma analizei cu privire la gradul de realizare a indicatorilor de criminalitate informatica, prestatorul va elabora un raport privind masurile si propunerile de optimizare a situatiei constatate la nivel national si comparativ cu situatia indicatorilor similari din Uniunea Europeana.

Prestatorul va urmari prin raportul sau sa propuna acele masuri de imbunatatire si aliniere a indicatorilor nationali la nivelul celor stabiliti prin analizele realizate de grupurile de lucru si expertii specializati in domeniul metodelor de combatere a criminalitatii informatice la nivelul Uniunii Europene.

Raportul trebuie sa sublinieze clar si concis rezultatele cercetarii, sistemetizate coerent cu marcarea diferentelor fata de situatia initiala studiata precum si evidentierea unor limite si sau dificultati.

Cerinte specifice

Ca prima etapa in cadrul acestei activitati, prestatorul va realiza o analiza calitativa asupra situatiei actuale in domeniul amenintarilor cibernetice la nivelul Romaniei.

Analiza calitativa a indicatorilor va trebui sa contina minim urmatoarele tipuri de elemente:

- Principalele amenintari de securitate cibernetica intalnite la nivelul Romaniei;
- Impactul amenintarilor cibernetice asupra mediului social si politic;
- Impactul amenintarilor cibernetice asupra mediului economic;
- Arii de importanta strategica nationala supra-expuse sau vulnerabile amenintarilor cibernetice;
- Trendul estimat in dezvoltarea amenintarilor de securitate cibernetica;
- Identificarea lacunelor legislative;

Ulterior analizei calitative a situatiei actuale in domeniul amenintarilor cibernetice la nivelul Romaniei, prestatorul va elabora un plan de dezvoltare si recomandari in domeniul securitatii cibernetice.

Planul de dezvoltare si recomandarile vor contine minim elemente de tipul:

- Masuri de prevenire a aparitiei si dezvoltarii de organizatii criminale de tip cibernetic;
- Politici de Early-Warning in domeniul securitatii cibernetice la nivel national;
- Politici de interventie si remediere in cazul unor atacuri cibernetice la nivel national;
- Masuri de colaborare institutionala;
- Masuri de incurajare a mediului academic, economic si social de a investi in domeniul securitatii cibernetice;
- Propuneri de colaborare internationala, in contextul accesului global la retelele informatice si a globalizarii criminalitatii cibernetice;

Livrabile

- document de analiza calitativa a indicatorilor de criminalitate informatica asupra situatiei actuale in domeniul amenintarilor cibernetice la nivelul Romaniei;
- plan de dezvoltare si recomandari in domeniul securitatii cibernetice;
- propunere de abordare legislativa din perspectiva liniilor directoare ce se impun a fi urmate din aceasta perspectiva.

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **400 de zile** de lucru.

4.5.2 Implementare soluție informatică (Activitatea 6 a proiectului)

În cadrul acestei activități se va dezvolta un sistem informatic integrat, compus din platforma hardware de bază și aplicațiile software necesare simulării diverselor tipuri de atacuri informatice și formulării tipurilor de măsuri de prevenire și de răspuns. De asemenea, vor fi instruiți 40 de utilizatori din cadrul CERT-RO și din cadrul echipelor formate folosind solutia informatica, în vederea dobândirii de cunoștințe practice privind funcționarea sistemelor implementate, precum și 3 administratori de sistem.

4.5.2.1 Analiză tehnică soluție informatică pe baza specificațiilor rezultate în urma fazei de analiză detaliată (Sub-activitatea 6.1)

Cerințe generale

În cadrul Sistemului Național de Combatere a Criminalității Informatice („Cyber Crime”) se va dezvolta un laborator de testare și instruire în domeniul securităţii cibernetice - denumit în continuare SISTEMUL (sau LABORATORUL DE TESTARE). Scopul sesiunilor de instruire în cadrul acestui LABORATOR, sub-adiacent scopului general al proiectului, constă pe de o parte în studierea celor mai răspândite si mai periculoase breșe și vulnerabilități de securitate ale diferitelor produse sau tehnologii informatice, iar pe de altă parte în propunerea celor mai potrivite măsuri de securitate, care să protejeze cât mai eficient sistemele informatice ale instituțiilor publice beneficiare.

SISTEMUL va avea următoarele caracteristici generale:

1) Va reprezenta o platformă tehnologică specializată, bazată pe o infrastructură hardware și software complexă, la standarde actuale, pentru pregătirea continua a specialiștilor din administrația publica în aspecte privind securitatea informatică.

2) Va crea un mediu tehnologic propice simulării unor tipuri de atacuri informatice şi formulării masurilor de prevenire si de răspuns în caz de incident cibernetic. Va permite de asemenea accesul cursanților la diverse aplicații de profil și instruirea acestora în diverse tehnici de atac și contracarare a atacurilor cibernetice.

3) Laboratorul va trebui să dispună de soluții de testare, scanare și simulare a diverselor tipuri de atacuri pentru diferite tipuri de sisteme informatice, de la cele de bază (sisteme de operare, servere email, servere de stocare etc.) la sisteme complexe (aplicații web, sisteme complexe de tip ERP/CRM bazate pe diferite tehnologii de programare, sisteme de tip DMS dezvoltate pe diferite tehnologii etc.). Sistemul trebuie să fie capabil să identifice vulnerabilitățile de securitate ale produselor sau tehnologiilor scanate, să elaboreze scenarii de atac și să propună măsuri pentru eliminarea vulnerabilităților sau stoparea atacurilor.

4) Sistemul trebuie să permită identificarea vulnerabilităților, elaborarea scenariilor de atac precum și furnizarea contramăsurilor necesare pentru o gamă largă de produse sau tehnologii informatice, astfel:

- Sisteme de operare.
- Sisteme de gestiune a bazelor de date.
- Servere web, incluzând diverse aplicații dezvoltate pe diverse tehnologii.
- Servere de email.
- Alte echipamente sau sisteme specifice mediului de rețea etc.

Cerinţe privind arhitectura sistemului

Soluția propusă de ofertant trebuie să conțină cel puțin următoarele componente, care integrate să poată constitui infrastructura informatică și de comunicații necesară pentru îndeplinirea scopului LABORATORULUI DE TESTARE și INSTRUIRE:

1) Platformă hardware de bază – echipamente hardware necesare funcționării sistemului.
2) Soluție integrată de virtualizare – soluție destinată folosirii optime a resurselor hardware disponibile.
3) Soluții de securitate specifice (scanare, testare, evaluare vulnerabilități etc.) – pentru identificarea vulnerabilităților, crearea scenariilor de atac și identificarea color mai bune măsuri de contracarare.

4) Echipamente de acces pentru administratorii de sistem

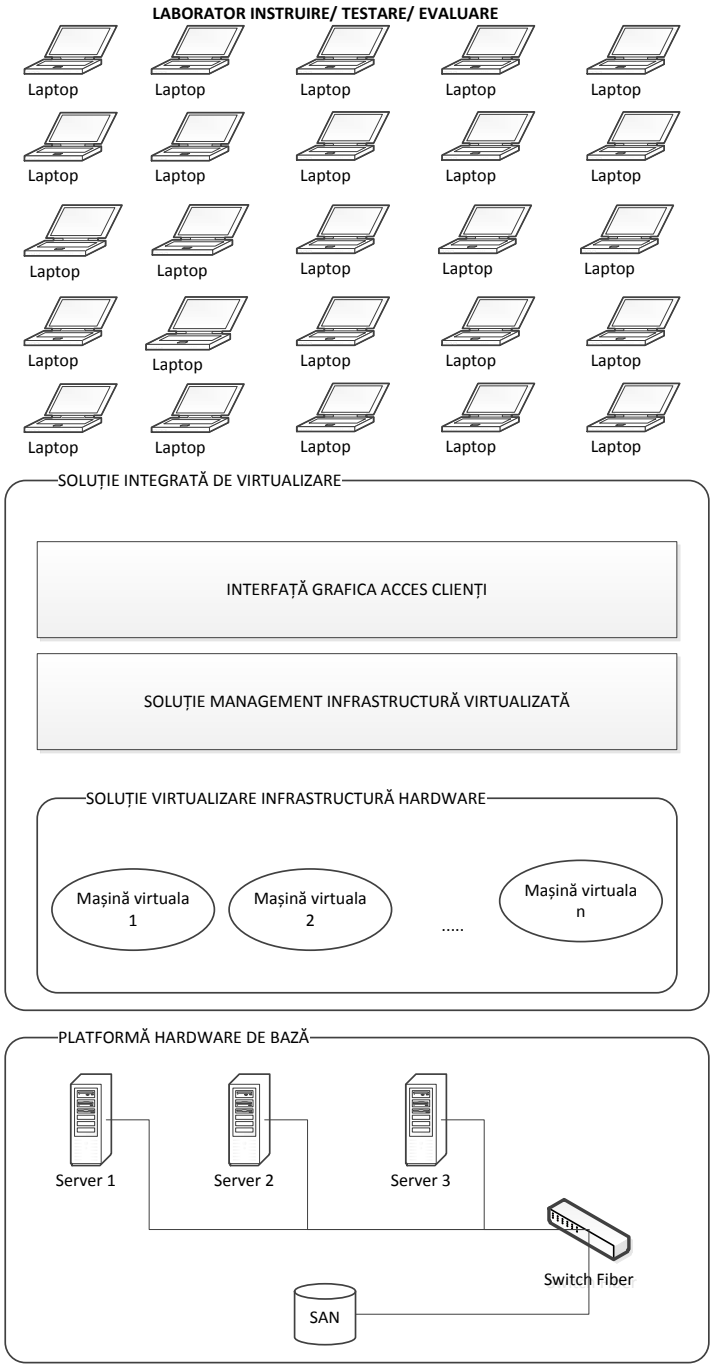

Figura 1 - Schema generică a soluției tehnice a proiectului

Descrierea detaliată a fiecărei componente enumerate mai sus se regăsește în subcapitolele de mai jos, iar schema arhitecturii sistemului se regăsește în figura 1.

Sistemul va oferi posibilitatea creării unor scenarii de atac informatic asupra a diferite produse sau tehnologii informatice. Astfel, pe platforma hardware de bază, gestionată prin intermediul soluției integrate de virtualizare, vor fi reproduse diverse scenarii de atac, respectiv configurații de sisteme informatice ce pot fi supuse unui atac informatic în lumea reală.

Soluția de virtualizare furnizată va trebui să fie compatibilă cu cele mai reprezentative sisteme de operare, pentru a asigura posibilitatea reproducerii unui număr relativ mare de tipologii sau configurații de sisteme informatice.

Se dorește ca scenariile de atac să poată fi modificate ulterior, în funcție de necesități, de evoluția produselor software sau chiar a metodelor de atac în sine, așadar soluția de virtualizare trebuie să suporte o gamă largă de sisteme de operare.

Soluțiile de securitate specifice sunt acele produse care vor permite cursanților să lanseze atacuri asupra sistemelor informatice (scenarii) reproduse în laborator. Soluțiile specifice vor permite într-o primă fază identificarea vulnerabilităților sistemului informatic. Apoi vor furniza diverse scenarii de atac, prin care să poată fi exploatate vulnerabilitățile identificate. Scenariile de atac trebuie sa fie prezentate într-o formă grafică, ușor accesibilă cursantului. Soluția, sau alte aplicații compatibile cu aceasta, trebuie să permită lansarea unor anumite atacuri, prin care să fie demonstrată existența vulnerabilităților identificate. De asemenea, solutia trebuie să fie capabila sa furnizeze contramăsuri pentru vulnerabilitățile identificate în cadrul produselor sau tehnologiilor scanate.

Pentru demonstrarea funcționalității sistemului, diverse scenarii vor fi puse în practică. Descrierea detaliată a cerințelor acestor scenarii va fi făcută ulterior în cadrul acestui caiet de sarcini.

Toate produsele livrate vor fi noi iar Prestatorul se va asigura de inter-compatibilitatea tuturor produselor și licențelor livrate în cadrul sistemului, precum și de livrarea tuturor sub-ansamblelor, licențelor, aplicațiilor și conecticii necesare funcționării întregului sistem, (inclusiv cabluri de conectare sau cabluri de alimentare etc.).

Livrabile

- Document de analiza functionala a cerintelor sistemului informatic;
- Document de cerinte tehnice a sistemului informatic;

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **175 de zile** de lucru.

4.5.2.2 Livrare platforma hardware de bază (Sub-activitatea 6.2)

Platforma hardware de bază este constituită din totalitatea echipamentelor, care asigură infrastructura informatică și de comunicații a sistemului. Platforma trebuie să suporte funcționarea tuturor aplicațiilor software prevăzute în prezentul caiet, de la soluția integrată de virtualizare la sistemele de operare solicitate.

Platforma hardware de bază este formată din următoarele componente:

- 1 dulap metalic (rack) de 19”
- 3 servere montabile în rack
- 1 switch fibre channel
- 2 switch-uri retea cu 24 porturi
- 1 echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată
- 1 soluție profesională de alimentare (UPS)
- 1 echipamente de stocare date

4.5.2.2.1 Cerinţe generale privind echipamentele

Toate cerintele tehnice sunt minimale si obligatorii.

Toate echipamentele ofertate trebuie sa fie compatibile cu standardele de alimentare cu energie electrica disponibile in Romania: 230V c.a. la 50 Hz.

Toate echipamentele ofertate trebuie sa fie noi si neutilizate.

Pentru fiecare echipament in parte se vor prevede accesoriile si cablurile de conexiunenecesare functionarii si interconectarii acestora , indiferent daca acestea au fost sau sunt sau nu expres solicitate.

Toate echipamentele trebuie livrate cu documentatie in limba romana sau engleza.

Pentru echipamentele hardware principale, ofertantii care nu sunt producatorii acestora, vor prezenta in cadrul ofertei o autorizatie de punere pe piata/de comercializare, emisa pe numele operatorului economic de catre fabricantii echipamentelor respective. Acest document trebuie sa fie emis cu maxim 30 zile inainte de data depunerii ofertei.

4.5.2.2.1.1 Cerinţe specifice dulap metalic (rack)

	Componenta	Specificații tehnice minimale și obligatorii
A.	**Înălțime utilă**	42U
B.	**Latime**	19”
C.	**Adancime**	≥ 1000mm, ≤ 1250 mm
D.	**Inaltime externă**	≤ 2100 mm
E.	**Capacitatea de încărcare statică**	≥ 600Kg
F.	**Standarde de conformitate**	EIA-310D, IEC 297
G.	**Usi fata/spate perforate**	Da
H.	**Panouri laterale detasabile**	Da
I.	**Securizare panouri laterale si usi fata/spate cu cheie**	Da
J.	**Solutie KVM**	- Consola LCD min. 17” , min. 250cd/m2, rack-mount si tastatura cu touchpad sau trackball - Switch KVM integrat cu 8 porturi compatibile cu servere furnizate

4.5.2.2.1.2 Cerinte specifice servere

	Componenta	Specificații tehnice minimale și obligatorii
A.	**Placa de baza**	Fabricata sub aceeasi marca cu sistemul de calcul
B.	**Format**	Rack-abil în rack-uri de 19’’ standard
C.	**Procesoare instalate**	2 x 8 cores Xeon min. 2.2 GHz, min.20 MB cache sau echivalent
D.	**Memorie**	96 GB DDR3 min.1333MHz. Min. 24 slot-uri de memorie disponibile pe server

E.	**Metode suporatate de protectie a memoriei**	Advanced ECC, Hot Spare Memory, SDDC
F.	**Hard-disk-uri interne**	2 x 300 GB SAS 10.000 rpm instalate intern. Discuri interne cu capabilitati de hot-swap cu posibiliate de upgrade la min. 8 discuri de tip SAS interne
G.	**Controller RAID**	Hardware cu capabilitate RAID 0 ,1, 5,6, 10 cu 512 MB memorie cache si protectie cu baterie
H.	**Sloturi de extensie**	7 sloturi de extensie de tip PCI-Express Gen.3
I.	**Interfete retea**	8 porturi 10/100/1000 Mbps Ethernet (dispuse pe minim 2 controllere diferite)
J.	**Interfete SAN**	2 porturi 8 Gbps Fibre Channel (dispuse pe HBA-uri diferite)
K.	**Conectori intrare/iesire**	6 x USB (min.2 porturi frontal), 2 x VGA (min. 1 port frontal), 1 x serial
L.	**DVD**	Unitate interna DVD-RW
M.	**Alimentare cu energie electrică**	2 x max.800 W, eficienta min.92% , redundante si de tip hot-swap
N.	**Ventilatoare**	Ventilatoare hot-swap si redundante
O.	**Management**	- port 10/100 Mbps dedicat (RJ45) pt administrare de la distanta - aplicatie pentru instalarea si configurarea serverului dezvoltata de producatorul serverului capabila de instalare locala si remote in mod neasistat, inclusiv configurare RAID; -aplicatie de management operational cu urmatoarele functii: monitorizarea starii sistemului, managementul evenimentelor si alarmelor, inventarul componentelor, inventarul si instalarea up-date-urilor si patch-urilor, analiza performantei, diagnoza on-line, restartarea si reconfigurarea automata a serverului, analiza si

		previzionarea defectarii componentelor; - chipset pentru remote management integrat compatibil IPMI 2.0 cu acces prin web browser cu securizare prin criptare SSL 128 bit, integrat cu aplicatia de management - posibilitatea de redirectionare a interfetei grafice si de accesare de la distanta a unitatilor de stocare interne si externe

4.5.2.2.1.3 Cerinte specifice switch fibre channel

	Componenta	**Specificații tehnice minimale și obligatorii**
A.	**Porturi totale**	24 x Fibre Channel
B.	**Porturi activate**	Minim 8 porturi activate si populate cu SFP-uri hot-plug, 8Gbit/s, conector LC
C.	**Performanta :**	Interfata port 8 Gbit/s, full duplex Latime de banda in mod agregat : minim 400 Gbit/s Suport pentru ISL Trunck, minim 60 Gbit/s
D.	**Tipuri de trafic de date**	Suport pentru UNICAST, MULTICAST şi BROADCAST
E.	**Accesorii :**	Switch-ul trebuie sa includa toate accesoriile necesare conectarii la servere, alimentarii cu energie electrica si instalarii in rack . Minim 8 cabluri MMF cu conectori LC-LC de minim 5 metri lungime

4.5.2.2.1.4 Cerințe specifice switch-uri rețea

	Componenta	Specificatii tehnice minimale si obligatorii
A.	**Cerinte generale cu privire la arhitectura si performante**	– Arhitectura non-blocking; – Minim 24 de porturi “10/100/1000Baset-T” RJ-45, – Minim 4 sloturi de tip “SFP”, cu transceiver-e Gigabit Ethernet pe fibra optica integrate; – Suport, prin dotare initiala sau prin upgrade ulterior, folosind module hardware dedicate, pentru interconectarea mai multor switch –uri intr-o arhitectura redundata, sub forma de unui singur switch, virtual, care sa aiba un singur management. Tehnologia de interconectare trebuie sa asigure: – viteza de transfer de minimum 20Gbps intre switch-uri; – Un numar de minim 4 switch-uri intr-un acelasi cluster; – Posibilitatea agregarii porturilor de pe switch-uri diferite prin protocol “LACP - Link Aggregation Control Protocol”, conform standardului IEEE802.3ad; – Capacitatea de comutare in backplane : minimum 175 Gbps – Capacitatea de procesare a traficului la nivelul unui sasiu: minimum 77 Mpps (Milioane pachete pe secunda) – Memorie RAM : minimum 128 MB – Memorie Flash : minimum 64 MB – Jumbo frames: pana la 9216 bytes – MTBF: minim 340.000 ore; – Echipamentul trebuie sa fie montabil in rack-uri standard de 19” si sa includa accesoriile necesare montarii
B.	**Sistem de operare**	– Sistemul de operare al echipamentului oferit va suporta urmatoarele standarde, conforme IEEE: – 802.1D MAC Bridges; – 802.1s Multiple Spanning Tree Protocol; – 802.1w Rapid Spanning Tree Protocol; – 802.3ad Link aggregation with LACP; – 802.3ab 1000BASE-T (10/100/1000 Ethernet over copper); – 802.3z Gigabit Ethernet; – 802.3ae 10 Gigabit Ethernet; – 802.1Q VLAN Tagging; – 802.1p Class-of-Service (CoS) Tagging for Ethernet frames; – 802.1x Port-based network access control. – Sistemul de operare al echipamentului va oferi urmatoarele facilitati Ethernet switching: – sistem de detectare a link-urilor unidirectionale; – protocol de propagare automata a VLAN-urilor; – posibilitatea blocarii traficului per port (unicast, multicast si

		broadcast); – PVRST+ (Per-VLAN Rapid Spanning Tree Plus) pentru interconectarea cu echipamentele existente ale beneficiarului – Sistemul de operare al echipamentului va oferi urmatoarele facilitati de securitate**:** – Liste de control al accesului si de filtrare a traficului la nivel de port; – Mecanism de segregare a traficului din acelasi VLAN, care sa restrictioneze comunicatia dintre hosturi apartinand aceleeasi retele IP; – Controlul accesului in retea bazat pe IEEE 802.1X; – Limitarea numarului de adrese MAC pe un port, prin mecanism “Port Security” sau echivalent; – Securizarea traficului DHCP prin mecanism “DHCP Snooping” sau echivalent; – Securizarea traficului ARP prin mecanism “Dynamic ARP Inspection” sau echivalent; – Prevenirea furtului sau a utilizarii neautorizate de adrese IP prin mecanism “IP source guard” sau echivalent; – Prevenirea interceptarilor de trafic si a perturbatiilor ce pot aparea intr-o retea ce foloseste Spanning Tree Protocol, prin mecanisme “Spanning Tree Root Guard” si “Bridge Protocol Data unit Guard” sau echivalent; – Sistemul de operare al echipamentului va oferi suport pentru QoS: – clasificare, marcare, limitare si plasare a traficului in cozi cu servire planificata; – minim 4 cozi de iesire per port; – coada de servire cu prioritate stricta (maxima) per port; – minim 64 de politici de limitare a traficului per port; – mecanisme de prioritizare bazate pe algoritmul “Shaped Round Robin” (SRR); – mecanisme de evitare a congestiei.
C.	**Alte cerinte**	– Inaltime maxima 1U – Fiecare switch va fi echipat cu cate 24 de patch-cord-uri de cupru de minim 5m lungime.

4.5.2.2.1.5 Cerinţe specifice echipament integrat de protecţie a reţelei ce funcţionează ca o soluţie de securitate unificată

	Componenta	Specificatii tehnice minimale si obligatorii
A.	Configurație	• 10 interfețe 10/100/1000 Ethernet • 1 port consolă
B.	Caracteristici	• Trafic firewall calculat pentru pachete UDP de 64 octeți, 512 octeți sau 1518 octeți: min. 8 Gbps • Trafic IPSec VPN (AES 256 SHA1): min. 6 Gbps • Trafic IPS pentru pachete UDP de 512 octeți: min. 800 Mbps • Trafic antivirus: min.160 Mbps • Trafic SSL VPN: min. 200 Mbps • Număr de clienți SSL VPN concurenți: min. 300 • Număr de tunele IPSec VPN concurente: min. 6000 • Număr de clienți IPSec VPN concurenți: min. 3000 • Număr de sesiuni concurente: min. 600000 • Număr de sesiuni noi pe secundă: min. 20000 • Număr de politici de securitate: min. 8000 • Număr de instanțe virtuale (mașini virtuale): min. 10 • Număr de utilizatori nelimitați • Spațiu de stocare local: 64GB

C.	Funcționalități generale	• Echipament integrat de securitate cu funcționalități simultane de:
		  • Firewall și firewall la nivel de aplicație de tip stateful - detectarea/blocarea aplicațiilor software
		  • Protecție antivirus
		  • Criptare de date: IPSec VPN și SSL VPN
		  • QoS și Traffic Shaping
		  • Detecția și prevenirea intruziunilor – IDS/IPS
		  • Scanare și filtrare WEB – Web Inspection/Filter
		  • Protecție antispam
		  • Protecție împotriva scurgerii de informații confidențiale
		  • Funcționalitate de proxy SSL – posibilitatea inspecției traficului criptat
		• Toate funcționalitățile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum și platforma hardware trebuie să aparțină aceluiași producător
		• Certificări pentru producător și produs: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs pentru: Firewall, IPSec, SSL, Network IPS, Antivirus
		• Conformitate cu CE, FCC Class A Part 15, UL/CUL, VCCI
		• Toate funcțiile trebuie să fie disponibile standard, indiferent de număr de utilizatori sau IP-uri
		• Soluția trebuie să fie de tip echipament hardware cu sistem de operare propriu dedicat funcționalităților de securitate necesare
		• Funcționalități NAT, PAT și Transparent Bridge

		• Opțiune de a aplica NAT per politică • Suport VLAN Tagging 802.1Q • Autentificarea utilizatorilor pe grupuri • Suport VoIP SIP/H.323/SCCP și Transversal NAT • Funcționalitate proxy explicit • Suport WINS • Suport securitate VoIP (SIP Firewall/RTP Pinholing) • Suport IPv6 (NAT/mod Transparent) • Politici de securitate bazate pe identitatea utilizatorului/servicii folosite • Opțiune “Scheduling” pentru politicile de firewall • Certificare ICSA Labs (Enterprise Firewall) • Optimizare de protocol (CIFS/FTP/MAPI/HTTP/HTTPS/TCP generic) • Compresie/decompresie în timp real a traficului (byte caching) • Caching prin proxy web transparent • Balansare de trafic pentru servere • Multiplexare TCP • Offloading pentru SSL (preia operațiunile de criptare/decriptare de la server-ul intern pentru HTTPS și execută aceste operații direct pe echipament) • Suport WCCP • Protecție anti-malware (virus, troian, worm, spyware) • Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, FTP, IM (AIM, ICQ, YAHOO, MSN) • Blocare după nume/tip/dimensiune fișier • Suport scanare antivirus Flow-Based • Filtrare pentru protocoalele HTTP și HTTPS • Filtrare după categorii site-uri/URL • Funcționalitate de contorizare a timpului de acces pentru utilizatori • Blocare a conexiunilor în funcție de URL/cuvânt cheie sau expresie în conținutul paginilor web • Filtrare pentru Java Applet, Cookies, Active X • Administrare prin WEB UI (HTTP/HTTPS), Telnet, Secure Command Shell (SSH) și Command Line Interface (CLI) • Utilizatori/Administratori cu drepturi configurabile • Funcționalitate de export/import a configurației • Politică de control a parolelor

4.5.2.2.1.6 Cerințe specifice soluție profesională de alimentare (UPS)

	Componenta	**Specificatii tehnice minimale si obligatorii**
A.	**Tehnologie**	Online Dubla Conversie
B.	**Putere iesire**	8KW/10 KVA
C.	**Tensiunea nominala iesire**	Configurabila 220V, 230V sau 240V
D.	**Tensiunea nominala intrare**	220V,230V sau 240V
E.	**Configurabil on site in urmatoarele moduri (intrare/iesire)**	1/1, 3/1
F.	**Frecventa tensiunii de intrare**	50/60 Hz +/- 3 Hz ; ajustabil+/- 0.1
G.	**Plaja variatie tensiune de alimentare fara comutare pe baterii**	160 - 280V
H.	**Randament la incarcare maxima**	92%
I.	**Factor creasta**	3:1
J.	**Forma de unda**	sinusoida pura
K.	**Factor distorsie THD intrare**	<7% la incarcare 100%
L.	**Tip conector iesire**	Hard wire plus 4 x IEC 320 C13, 4 x IEC 320 C19
M.	**Cabluri consumatori**	DA, 4 buc
N.	**Bypass**	Da, baypass intern (manual si automat)
O.	**Montare rack UPS**	DA, maxim 9U inclusiv cabinetul suplimentar de baterii
P.	**Timp de functionare la incarcare maxima**	minim 4 minute
R.	**Interfata**	DB-9 RS-232,RJ-45 10/100 Base-T
Q.	**Card de retea**	DA, preinstalat si cu sensor de temperatura

S.	**Afisaj LED**	DA
T.	**Alarme sonora si vizuala**	DA

4.5.2.2.1.7 Cerinţe specifice echipament stocare

	Componenta	**Specificatii tehnice minimale si obligatorii**
A.	**Descriere :**	– Echipament de stocare cu arhitectura redundanta. Sistemul trebuie sa fie echipat cu doua controlere capabile de redundanta si failover automat. – In configurația propusa sistemul va fi livrat cu ambele unităţi de tip controller instalate.
B.	**Scalabilitate:**	– Modelul ofertat trebuie sa suporte minim 120 discuri. – Sistemul trebuie sa ofere o scalabilitate de minim 240 discuri, fara a fi necesara migrarea datelor.
C.	**Conectivitate :**	– Sistemul trebuie sa fie echipat cu minim 8 porturi FC 8GB/s, instalate si functionale, cu SFP-urile aferente incluse. – Sistemul trebuie sa suporte interfete de conectare cu porturi iSCSI 10GB/s si FCoE 10GB/s. – Sistemul trebuie sa ofere posibilitatea de intermixare a diferitelor tipuri de porturi la nivel de controler.
D.	**Memorie cache:**	– Minim 2GB memorie cache per controler. – Memoria cache trebuie sa dispuna de un mecanism de protectie ECC. – Sistemul trebuie sa dispuna de o memorie nevolatila de tip Flash pentru asigurarea protectiei datelor din memoria cache, in cazul opririi neprogramate a sistemului de stocare . Retentia datelor din memoria cache trebuie sa se realizeze pentru o perioada nelimitata de timp.
E.	**Discuri pentru date :**	– In configuratia solicitata sistemul trebuie sa fie

		echipat cu minim 12 x 450 GB, 15.000 RPM, SAS – Sistemul trebuie sa suporte discuri de mare capacitate: minim 900GB SAS, minim 3TB NL-SAS/SATA, minim 400GB SSD. – Posibilitate de intermixare in cadrul aceluiasi sertar de discuri, cel putin a urmatoarelor tehnologii de disc: SSD, SAS, NL-SAS/SATA. – Sistemul trebuie sa permita atat discuri de 3.5 inch cat si de 2.5 inch , hot-swappable. – Sistemul trebuie sa permita intermixarea unitatilor de expansiune cu discuri de 3.5” cu cele de 2.5”.
F.	**RAID:**	– Suport pentru RAID : 0, 1, 10, 5, 50, 6. – Sistemul de stocare trebuie să permită refacerea on-line a nivelurilor RAID. – Sistemul trebuie sa dispuna de un mecanism de monitorizare proactiva a starii discurilor si de recuperare a datelor in cadrul grupului RAID. Acest mecanism trebuie sa ofere posibilitatea recuperarii datelor cu ajutorul unui disc de spare, inainte de caderea efectiva a unui disc de date. – Sistemul trebuie sa permita atat discuri de spare dedicate cat si globale.
G.	**Suport pentru servere host :**	– Sistemul trebuie sa suporte fara alte costuri de licentiere minim 100 servere host – Sistemul trebuie sa ofere suport pentru minim 2000 LUNs. – Sistemul trebuie sa ofere suport pentru LUN-uri cu capacitate de minim 100TB.
H.	**Management:**	– Software de management, configurare a sistemului si a căilor de acces catre serverele host, fabricat de același producător si inclus in configurația de baza a echipamentului. – Interfata WEB, CLI SMI-S, aplicatia de management trebuie sa permita definirea mai multor nivele de utilizator pentru administrarea sistemului. – Facilitati pentru mentenanta sistemului: notificari E-

		mail, Wake On LAN, SSL/SSH. – Aditional, sistemul de stocare trebuie sa ofere un nivel de administrare centralizata impreuna cu sistemele server, printr-o unica aplicatie de management, fabricata de acelasi producator.
I.	**Disponibilitate:**	– Upgrade-urile de firmware trebuie sa se poata face online, fara oprirea sistemului . – Surse de alimentare si ventilatoare redundante in tehnologie hot swap. – Integritatea datelor trebuie sa fie garantata, atat in memoria cache cat si la nivel de disc, prin detectia erorilor la nivel de block, printr-un mecanism de tip check code.
J.	**Facilitati software :**	– Sistemul trebuie sa ofere posibilitatea de migrare a datelor intre diferite grupuri RAID, in maniera online, fara a intrerupe operatiunile.
K.		– Sistemul trebuie sa permita marirea numarului de HDD-uri dintr-un grup RAID prin adaugarea de noi disc-uri, in maniera online , fara intreruperea operatiunilor.
L.		– Sistemul trebuie sa permita criptarea datelor, posibilitatea de a activa aceasta functionalitate la nivel de volum. Functionalitatea trebuie să fie suportata la nivel de controler fără utilizarea unor subansamble externe sistemului de stocare.
M.		– Sistemul trebuie sa suporte oprirea programata a rotatiei discurilor daca acestea nu sunt in utilizare, ca masura de reducere a consumului de energie electrica. Operatiunea trebuie sa se realizeze in conditiile pastrarii timpilor de acces optimi la date.
N.		– Sistemul trebuie sa suporte facilitatea de Thin Provisioning, mecanismul trebuie sa permita alocarea către servere a unor capacitați virtuale mai mari decât cele instalate fizic in interiorul sistemului de

		stocare. Facilitate disponibila eventual prin licentiere interioara.
O.		– Sistemul trebuie sa permita realizarea a minim 1000 sesiuni de copiere instanee de tip Snapshot.
P.		– Sistemul trebuie sa permita acces redundant la sistemele host, si sa includa drivere multipath cel putin pentru urmatoarele sisteme de operare : MS Windows , Linux, IBM AIX, SUN Solaris
R.	**Performanta :**	– Sistemul ofertat trebuie sa fie testat Benchmark SPC-1 sau echivalent, si sa suporte performanta de minim 33.000 IOPS

4.5.2.2.2 Cerinţe soluţie integrată de virtualizare

Soluția integrată de virtualizare (SIV) are rolul de a transforma platforma hardware într-o infrastructură virtuală agregată și scalabilă cu scopul folosirii eficiente a resurselor de calcul și oferirii de servicii într-un mod mult mai flexibil decât prin variante tradiționale.

Soluția propusă de ofertant trebuie să înglobeze un hypervizor independent de platformă care să aibă posibilitatea de virtualizare a infrastructurii hardware (echipamente de procesare, echipamente de stocare și echipamente de comunicații), o interfață user-friendly de management al mediului virtualizat și interfețe de acces pentru utilizatorii sistemului.

Soluţia integrată de virtualizare trebuie să satisfacă următoarele cerinţe şi caracteristici tehnice minimale:

- Să permită virtualizarea și partajarea resurselor/componentelor fizice de stocare, procesare și rețea
- Hypervisor de nivel 1 – un hypervisor care rulează imediat deasupra platformei hardware a Host-ului, fără a avea nevoie de un sistem de operare intermediar (soluţie cunoscută în literatura de specialitate şi ca mediu de virtualizare de tip “bare metal”)
- Sa permita rularea pe servere fizice ce contin ce contin pana la 160 coruri logice de procesare si 2048 GB memorie fizica
- Sa asigure concomitent pentru o singura masina virtuala configurarea cu 32 procesoare virtuale si 1024 GB RAM, resurse care vor putea fi folosite efectiv in limitele de adresare impuse de sistemul de operare virtualizat
- Platforma de virtualizare trebuie sa fie independent de metoda de stocare interna/externa a serverului/serverelor pe care ruleaza
- Sa suporte diverse tipuri de storage (SAN, NAS, iSCSI) si protocoale de access (FC, FCOE, ISCSI, NFS) si sa permita prioritizarea si garantarea performantelor I/O (SLA) ale masinilor virtuale, la nivel de cluster

- Accesul către sistemul de stocare extern sa poată fi făcut pe mai multe căi (multipathing), asigurându-se suport pertru fail-over si load balancing şi având posibilitatea de alegere a politicii de stabilire a căii (fixă, MRU, Round Robin)
- Sistemul de fişiere va permite accesul concurent a mai multor servere fizice (host) şi a mai multor maşini virtuale la aceeaşi resursă de stocare
- Sistemul de fişiere trebuie să asigure că o maşină virtuală este accesată doar de pe un singur host (sistem de blocarea accesului); în caz de defectare a host-ului maşina virtuală trebuie să poată fi restartată de pe alt server fizic;
- Sistemul de fişiere va asigura posiblitatea migrării în timp real (fără intreruperea funcţionării) unei maşini virtuale de pe un host pe altul, de pe o capacitate de stocare pe alta
- Sistemul de fişiere tebuie să suporte expansiunea dinamcă a volumelor şi LUN-uri de peste 2TB
- Sa se poata face administrarea platformei virtuale atat prin interfata de tip consola, local sau de la distanta, cat si prin browser web si prin platforma de management dedicata
- Componentele platformei hardware virtuale, asa cum sunt acestea prezentate sistemelor de operare din masina virtuala, sa poata fi modificate cu usurinta (adaugare/eliminare) ;
- Sa prezinte capacitate de a forma un cluster tolerant la defectiunile nodurilor scalabil pana la 32 noduri
- Sa permita restartarea automata , fara interventie umana, a masinilor virtuale care rulau pe un nod al cluster-ului care s-a defectat, pe celelalte noduri ramase in cluster
- Functionalitate de a muta masinile virtuale intre hosturi automat si manual(fara intreruperea serviciilor catre utilizatori)
- Functionalitate de a asigura persistenta “statefull” a aplicatiilor chiar si in cazul defectiunilor hardware si in cazul migrarilor neplanificate de pe un host pe celalalt
- Capabilitate de “NIC teaming” pentru placile de retea, cu sistem de distributie a traficului automat intre interfete in functie de incarcare
- Sa aiba suport pentru instalarea in masini virtuale (cel putin) oricare dintre urmatoarele sisteme de operare :
    - Windows Xp/Vista/7/2003/2008/2008 R2,
    - Linux Suse/Red Hat/CentOS,
    - FreeBSD,
    - Solaris
    - Netware.
- Filesystem propriu de performanta inalta optimizat pentru lucrul in mediu virtual
- Sa permita mutarea masinilor virtuale de pe un server pe altul fara oprirea sistemului de operare ce ruleaza in masina virtuala si fara intreruperea serviciului oferit de aplicatia/aplicatiile din masina virtuala ;
- Sa permita consolidarea masinilor virtuale - in mod automat, prin politici predefinite, sau manual - pe un numar prestabilit de servere si sa opreasca automat serverele fara activitate sau cu sub-utilizare a resurselor de procesare
- Software-ul instalat pe host trebuie să poată crea echipamente de reţea virtuale (switch-uri) la care să se conecteze maişinile virtuale şi interfetele de retea fizice de pe host;

- Sa permită realizarea de switch-uri virtuale distribuite pe mai mute host-uri si sa ofere interfete de programare pentru aplicatii (API) pentru switch-uri virtuale distribuite de alti producatori.
- Sistem de QoS la nivel de retea si capacitate de stocare, pentru a prioritiza traficul de date si accesele in storage
- Firewall integrat care poate oferi functii de raportare, analiza si configurare restrictii de trafic la nivel de protocol intre masinile virtuale
- Sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati
- Sa permita balansarea dinamica automata/manuala a resurselor de procesare existente in platforma virtuala in functie de necesitati si/sau pe baza unor reguli/politici prestabilite
- Sa balanseze automat incarcarea intre hosturi, pentru a optimiza consumul de curent, si care sa poata opri automat anumite hosturi neutilizate
- Aplicatia trebuie sa ofere suport pentru aplicarea centralizata a actualizarilor (patch-urilor) pentru host-uri
- Aplicatia de virtualizare trebuie sa permită managementul salvărilor contextuale (snap-shot) ale maşinilor virtuale; astfel incat o maşină virtuală se va putea restaura din orice salvare anterioară
- Sistem de management centralizat realizat de producatorul software-ului de virtualizare care sa acopere toate sistemele de mai sus care sa asigure:
    - Definirea si aplicarea de profile de configuratie standard pentru serverele ce fac parte din infrastructura virtuala.
    - Sistem de inventariere complet pentru masini virtuale, resurse storage, memorie, CPU, etc.
    - Generare interactiva de harti cu structura topologiei
    - WebAccess pentru managementul sistemului
    - Monitorizarea sistemului (host-uri si masini virtuale). Grafice de performanta
    - Sistem de alertare si notificari bazate pe alarme
    - Sistem integrat de patch management (hosturi si masini virtuale)
    - Sistem integrat de conversie a masinilor fizice in masini virtuale
    - Separarea privilegiilor administrative in functie de roluri predefinite/definibile
    - configurarea, pornirea si oprirea masinilor virtuale
    - managementul licentelor achiziţionate
    - sistem de control al accesului diferenţiat,bazat pe roluri pentru diferite grupuri de utizatori;
    - monitorizarea activtăţii serverelor şi maşinilor virtuale (memorie alocată, încărcarea procesoarelor, traficul de retea, etc.)
    - sa ofere impementarea centralizata a update-urilor pentru hypervizor
- Servicii de suport direct de la producatorul aplicatiei de virtualizare, si de actualizare si upgradare automata in cazul in care apar versiuni noi, pentru o perioada de 12 luni de la achizitia licentelor.
- Solutia va fi licentiată pentru toate serverele oferite si pentru toate resursele de procesare ale serverelor oferite si pentru cel putin o instantă de nod (fizic sau virtual) de management al intregii infrastructuri virtualizate.

4.5.2.2.3 Cerinţe echipamente acces administratori

Urmatoarele echipamente vor fi furnizate pentru administratorii sistemului:

- 3 laptopuri pentru administratorii de sistem

4.5.2.2.3.1 Laptop administratori: 3 buc

	Componenta	**Specificatii tehnice minimale si obligatorii**
A.	**Placa de baza**	Fabricata sub aceeasi marca cu sistemul de calcul
B.	**Display**	14”, LED backlight , minim 1366 x 768 pixeli
C.	**Procesor**	Minim Procesor Intel Core i5 cu 2 nuclee de procesare si cel putin 4 threads disponibile sau echivalent Frecventa procesor : min 2.2 GHz Cache: min 3MB
D.	**Chipset**	Intel QM77 sau echivalent
E.	**Memorie ram**	4 GB DDR3 cu posibilitatea de extindere la 16 GB
F.	**Tastatura**	Tip Qwerty rezistenta la stropiri accidentale
G.	**Mouse**	Touch pad cu 2 butoane si scroll
H.	**Hard disk**	500 GB SATA cu senzor de soc
I.	**Unitate optica**	DVD-RW
J.	**Placa video**	Integrata
K.	**Placa audio**	Integrata
L.	**Conectivitate**	Integrata 10/100/1000 Gigabit Ethernet, WLAN 802.11b/g/n
M.	**Interfete integrate (fara adaptori)**	- 2 x USB 3.0 - 2 x USB 2.0 (din care minim 1 port prezinta posibilitatea de incarcarea a dispozitivelor mobile chiar si cu laptop-ul oprit) - 1 x Audio out - 1 x Audio in - 1 x Microphone

		- 1 x RJ45 - 1 x VGA - 1 x Display Port - 1 x Express Card Slot - 1 x Card Reader (formate suportate cel putin SD, SDHC si SDXC)
N.	**Caracteristici de securitate**	- Suport pentru incuietoare de tip Kensington Lock (se va livra si nu cablu tip Kensington pentru securizarea laptop-ului) - BIOS compatibil Computrace - Parola pentru acces utilizator si BIOS
O.	**Management**	WoL (Wake on LAN), WMI,PXE,iAMT V7.0, vPro sau echivalent Aplicatie de management local si de la distanta dezvoltata de producatorul sistemului de calcul, cu cel putin urmatoarele functionalitati : - Management de la distanta atat online cat si offline - Rapoarte detaliate despre componentele sistemului - BIOS Management
P.	**Software preinstalat de la producatorul echipamentului**	Utilitare pentru managementul energiei si retelei Utilitar pentru restaurarea imaginii sistemului
Q.	**Conformitate cu standardele**	RoHS CE Energy Star 5.0
R.	**Autonomie**	Pana la 12 ore cu bateria furnizata (testare conform BAPCO Mobile Mark 2007)
S.	**Greutate**	Maxim 2.5 kg

T.	**Accesorii**	Geanta transport , hard disk portabil minim 1TB cu interfata USB 3.0 si stick de memorie USB minim 32 GB cu interfata USB 3.0

- **Livrabile:** Echipamente hardware si manualele de instructiuni aferente:
  - 1 dulap metalic (rack) de 19”
  - 3 servere montabile în rack
  - 1 switch fibre channel
  - 2 switch-uri retea cu 24 porturi
  - 1 echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată
  - 1 soluție profesională de alimentare (UPS)
  - 1 echipamente de stocare date
  - 1 solutie de virtualizare
  - 3 laptopuri administratori
- Proces verbal de predare primire a echipamentelor hardware;

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **0 zile** de lucru.

4.5.2.3 Instalare echipamente hardware (Sub-activitatea 6.3)

Laboratorul va trebui livrat la cheie de către ofertant, respectiv echipamentele hardware trebuie sa fie instalate și puse în funcțiune după specificațiile beneficiarului. Următoarele activități vor trebui întreprinse în cadrul acestei etape:

- Instalare, configurare și operaționalizare platforma hardware achiziționata (laboratorul)
  - Solutia integrata de virtualizare se doreste instalata pe platforma hardware furnizata. Se doresc configurate un numar de 8 masini virtuale (scenarii de testare) pe baza specificatiilor ulterioare formulate de echipa tehnica a proiectului

Livrabile

- Document sumar de instalare si configurare echipamente hardware;

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **20 de zile** de lucru.

4.5.2.4 Proiectare si programare solutie (Sub-activitatea 6.4)

Prestatorul va asigura implementarea sistemului informatic compus din aplicatii necesare simularii diverselor tipuri de atacuri informatice si formularii tipurilor de masuri de prevenire si de raspuns.

Platforma software trebuie sa contina cel putin urmatoarele module:

- Solutie securitate de baza pentru modele de retea, firewall assurance, network assurance si risk control
- Solutie pentru simularea atacurilor Cyber
- Solutie mobila de testare pentru echipamentele mobile instalat pe echipamente specifice

4.5.2.4.1 Software securitate de baza

- Solutia trebuie sa permita realizarea a cel putin 3 modele ale retelei, independente intre ele.
- Solutia trebuie sa permita trimiterea de notificari pe email in functie de anumite evenimente.
- Solutia trebuie sa includa un sistem intern de tichete.
- Solutia trebuie sa includa un sistem de baze de date intern, pe care sa fie folosit pentru stocarea configuratiilor echipamentelor din retea, fara a fi necesara instalarea unui sistem de baze de date separat de solutie.
- Solutia trebuie sa ofere un framework care sa permita importul de date si din alte surse decat cele suportate in mod direct.
- Solutia trebuie sa se prezinte sub forma unei aplicatii software.

Capabilitatea de firewall assurance

- Solutia trebuie sa ofere suport pentru o gama larga de vendori de firewall-uri.
- Solutia trebuie sa permita colectarea configuratiilor echipamentelor atat manual, cat si in mod automat (planificat), atat prin preluarea unor fisiere de configuratie salvate anterior, cat si prin conectarea la dispozitiv.
- Solutia trebuie sa realizeze o normalizare a configuratiilor, pentru a le prezenta in tr-un mod unitar.
- Solutia trebuie sa permita stabilirea de zone pentru interfetele echipamentelor.
- Solutia trebuie sa permita o reprezentare grafica a conexiunilor firewall-urilor.
- Solutia trebuie sa ofere posibilitatea verificarii configuratiei echipamentelor conform unor politici de acces, politici privind structura regulilor si unor cerinte de bune practici.

- Solutia trebuie sa permita verificarea conformitatii configuratiei firewall-urilor cu politicile de acces in functie de zonele alocate pentru interfetele acestora.
- Solutia trebuie sa ofere politici de acces (NIST si PCI) si de bune practici prestabilite pentru verificarea configuratiei firewall-urilor.
- Solutia trebuie sa ofere posibilitatea indentificarii regulilor nefolosite.
- Solutia trebuie sa permita identificarea regulilor “shadowed” si a celor redundante.
- Solutia trebuie sa permita identificarea regulilor care nu sunt jurnalizate.
- Solutia trebuie sa permita realizarea de comparatii intre configuratiile firewall-urilor din acelasi model al retelei si din modele diferite
- Interfata de management trebuie sa permita exportul tabelelor afisate in format CSV.
- Solutia trebuie sa ofere posibilitatea identificarii modificarilor aduse configuratiei unui firewall.
- Solutia trebuie sa contina un sistem de management al modificarilor care sunt aduse firewall-urilor.
- Solutia trebuie sa ofere posibilitatea realizarii de rapoarte atat pentru fiecare firewall in parte, cat si pentru toate firewall-urli analizate.
- Solutia trebuie sa asigure structuri de rapoarte predefinite, dar si posibiltatea definirii unor noi structuri de rapoarte.

Capabilitatea de network assurance

- Solutia trebuie sa ofere suport pentru o gama larga de vendori (Juniper, Checkpoint, Cisco, Brocade, Baracuda, Fortinet, Nortel, Palo Alto, McAfee)
- Solutia terbuie sa realizeze o normalizare a configuratiilor nodurilor de retea pentru a le prezenta in mod unitar.
- Solutia trebuie sa permita realizarea unui reprezentari grafice a retelei. Reprezentarea grafica trebuie sa poata fi rearanjata, afisata pe sectiuni, sa se poata scoate in evidenta diverse elemente din cadrul sau si sa poata fi exportata ca de tip imagine sau ca fisier pentru Visio (vdx).
- Solutia trebuie sa permita verificarea conformitatii accesului in retea cu politici de acces.
- Solutia trebuie sa ofere politici de acces prestabilite pentru verificarea conformitatii retelei
- Solutia trebuie sa permita verificarea configuratiei echipamentelor analizate in baza unor politici de bune practici.
- Solutia trebui sa furnizeze politici de acces si de bune practici predefinite, dar si posibilitatea de a modifica aceste politici si de a defini altele noi.
- Solutia trebuie sa permita verificarea accesului intre diferite zone ale retelei si sa afiseze garfic traseul urmat. In cazul in care accesul este impiedicat sa permita identificarea cauzei care blocheaza accesul (ex. Regula de firewall care nu permite accesul).

- Solutia trebuie sa asigure structuri de rapoarte predefinite, dar si posibiltatea definirii unor noi structuri de rapoarte.

Capabilitatea de risk control

- Solutia trebuie sa permita importul de date privind vulnerabilitatile din urmatoarele scanere de vulnerabilitati: QualysGuard, Tenable Nessus, NMAP Network Scanner, eEye REM, Rapid7 NeXpose, McAfee Vulnerability Manager, IBM Proventia Network Enterprise Scanner
- Solutia tebuie sa permita importul datelor despre versiunile sistemelor de operare si ale aplicatiei instalate din Microsoft SCCM si stabilirea vulnerabilitatilor aferente acestora fara a fi nevoie de efectuarea unei scanari cu un scaner de vulnerabilitati.
- Solutia trebuie sa permita definirea amenintarilor la adresa echipamentelor din retea.
- Solutia trebuie sa identifice caile posibile de atac din cadrul retelei, tinand cont de topologia retelei.
- Solutia trebuie sa poata identifica vulnerabilitatile care nu sunt expuse direct unei amenintari, dar care pot fi exploatate printr-un atac in mai multi pasi si sa calculeze riscul pentru echipamentele care contin aceste vulnerabilitati in concordanta.
- Solutia trebuie sa ofere posibilitatea de a vizualiza grafic atacurile posibile, atat cele asupra vulnerabilitatilor expuse direct, cat si cele in mai multi pasi, oferind informatii despre echipamentele implicate, vulnerabilitatile exploatate si ruta in interiorul retelei folosita de atacator.
- Solutia trebuie sa permita creare de tichete pentru remedierea vulnerabilitatilor in timpul explorari grafice a unui atac.
- Solutia trebuie sa permita calcularea mai multor indicatori de performanta (KPI).
- Solutia trebuie sa permita realizarea de analize asupra modelului retelei pentru gruparea echipamentelor, vulnerabilitatilor si amenintarilor in functie de anumite criterii.
- Solutia trebuie sa furnizeze solutii pentru vulnerabilitatile prezente in retea.
- Solutia trebuie sa asigure structuri de rapoarte predefinite, dar si posibiltatea definirii unor noi structuri de rapoarte.

4.5.2.4.2 Soluţie software pentru simularea atacurilor Cyber

Se doreste o solutie software capabila sa evalueze proactiv sistemele IT in raport cu amenintarile din lumea reala. Solutia trebuie sa realizeze teste:

- Pentru penetrare retea
- Pentru securitatea aplicatiilor web
- Pentru vulnerabilitatile dpdv statii de lucru
- Pentru securitatea retelelor wireless
- Pentru echipamentele mobile

Solutia trebuie sa fie capabila sa realizeze atacuri care parcurg aplicatii web, sisteme de retea, clienti finali, utilizatori de email, retele Wifi, retele si dispozitive mobile.

Solutia trebuie sa puna la dispozitia utilizatorilor o biblioteca mare de exploit-uri comerciale disponibile, completata cu un set complet de intrumente necesare inainte si dupa compromiterea unui sistem.

Solutia trebuie sa ofere o gama larga de rapoarte care sa permita identificarea vulnerabilitatilor critice si prioritizarea remedierii acestora.

Solutia trebuie sa fie mereu actualizata si conectata cu noile exploit-uri si module de securitate.

Sisteme suportate

Soutia trebuie sa fie suportata in mod obligatoriu cel putin pe urmatoarele platforme:

- Windows 7 Ultimate SP1(32 sau 64 bits)
- Windows 7 Professional SP1 (32 sau 64 bits)
- Windows XP Professional SP3

Interfata cu utilizatorul

Solutia trebuie sa asigure utilizatorului urmatorele metode de interactiune pentru:

- Configurarea si pregatire testelor cu ajutorul unui vrajitor.
- Selectia si executarea automata a exploit-urilor.
- Posibilitatea de a selecta si executa exploit-uri individuale
- Posibilitatea de a programa cand sa fie rulate testele
- Posibiltati de a crea fluxuri de testare particularizate
- Posibilitatea de a particulariza solutia si exploit-urile
- Posibilitatea de a scrie si de a rula propriile exploit-uri, folosind solutia.

Teste pentu penetrarea retelei

Solutia trebuie sa identifice si sa stabileasca caracteristicile sistemelor dintr-o gama de adrese IP data.

Solutia trebuie sa ofere o varietate de metode pentru identificare echipamentelor din retea si pentru scanarea porturilor.

Solutia trebuie sa permita importul rezultatelor din multiple scanere de vulnerabilitati si sa valideaze rezultatele din punct de vedere al exploatabilitatii.

Solutia trebuie sa poata testa echipamente care ruleaza urmatoarele sisteme de operare:

- Windows (32 & 64-bit)
- Linux
- Mac OS X
- AIX

- Sun Solaris
- OpenBSD

Solutia trebuie sa evalueze securitatea sistemelor IPv6.

Solutia trebuie sa permita testarea ruterelor si switch-urilor.

Exploit-urile noi si actualizarile trebuie sa fie disponibile in mod regulat

Exploit-urile prezente in cadrul solutiei trebuie sa poata fi particularizate.

Codul trimis de catre exploit-uri trebuie sa asigure, pe timpul testarii, o interfata catre sistemele compromise pentru a se putea stabili implicatiile compromiterii sistemului respectiv. Se cer functionalitati ca:

- Vizualizarea structurii de fisiere existent pe masinile compromise si a continutului acestora.
- Vizualizarea drepturilor obtinute pe masina compromisa
- Realizarea de capturi ale imaginilor de pe ecran
- Intercatiunea cu masina compromisa in linie de comanda
- Colectarea parolelor si a fisierelor cookie

Codul trimis de exploit-uri trebuie sa asigure accesul la apelurile de sistem si API-urile sistemului de operare Windows.

Codul transmis de catre exploit-uri trebuie sa suporte plug-in-uri binare si cod.

Codul trimis de exploit-uri treuie sa suporte metode de conectare multiple.

Solutia trebuie sa fie capabila sa mentina comunicarea cu sistemele compromise atunci cand aceste sunt repornite.

Solutia trebuie sa permita evaluarea posibilitatilor unui atacator de a obtine privilegii administrative pe sistemele compromise.

Solutia trebuie sa ofere posibilitatea de a trece de la un sistem compromis la altul pentru a simula incercarile unui atacator in cadrul retelei.

Solutia trebuie sa poata rula aplicatii ale unor terte parti impotriva sistemelor compromise, in timpul testelor. Solutia trebuie sa permita:

- stabilirea de puncte de conexiune VPN catre agentii care ruleaza pe masinile compromise, atat pe tinte Windows, cat si pe Linux
- rularea aplicatiilor celor terte parti prin intermediul acestor puncte de conexiune VPN

Solutia trebuie sa nu lase nici un fel de cod pe sistemele testate, dupa terminarea testelor. De asemenea, se doreste ca toate activitatile de curatare sa fie inregistrate in fisierele de jurnalizare ale solutiei.

Teste pentru securitatea aplicatiilor web

Solutia trebuie sa aiba capabilitati automate de parcurgere a site-uilor web pentru a identifica paginile web care urmeaza a fi testate. Utilizatorul trebuie sa poate specifica numarul maxim de pagini care sa analizat si adancimea maxima pana la care sa fie parcurs un site. De asemenea se poate specifica un navigator web care sa fi impersonat de solutie.

Solutia trebuie sa fie capabila sa descopere aplicatii web pe serverele HTTP.

Solutia trebuie sa permita evaluarea vulnerabilitatilor existente in codul javascript.

Solutia trebuie sa ofere posibilitatea testarii vulnerabilitatilor aplicatiilor web prezente in OWASP Top 10.

Solutia trebuie sa testeze pentru posibilitatea includerii atit local cat si de la distanta a fisierelor cu cod malitios.

Solutia trebuie sa poata testa posibilitatea de Cross-Site Scripting in obiectele Adobe Flash.

Optiunea de web application penetration testing trebuie sa ofere celor care folosesc solutia posibilitatea de a evalua implicatiile unei brese intr-o aplicatie web. De exemplu posbilitatea de identificare a datelor supuse riscului in cazul unei vulnerabilitati sau in cazul unui atac al carui tinta sa fie o retea back-end.

Teste pentru vulnerabilitatile statiilor de lucru

Solutia trebuie sa includa capabilitati automate de colectarea a aderselor de e-mail si alte informatii publice in scopul folosirii lor in cadrul testelor.

Capabilitatea de colectarea a informatiilor vizand partea de statii de lucru a solutiei trebuie sa poata colecta in mod automat adrese de e-mail din urmatoarele surse:

- Locatii publice utilizand Google, Yahoo, Altavista, Bing, Metacrawler, Ask, si About
- Baze de date publice, din internet, incluzand PGP, DNS si WHOIS
- Descoperire (crawling) in site-uri web

De asemenea se doreste optiunea exportului adeselor de mail folosite in cazul testelor in format CSV sau TXT.

Solutia trebuie sa aiba optiunea identificarii credit card-urilor sau CNP-uri ce ar putea fi expuse de catre utilizatori atit in site-uri web cat si in documentele postate on-line.

Solutia trebuie sa aiba abilitatea de a testa atit vulnerabilitatile in multe aplicatii client precum si modul in care pot fi ele exploatate.

Solutia trebuie sa aiba posibilitatea replicarii atacurilor ce pot rezulta din atasamente e–mail malitioase sau care ar rezulta de pe drive-uri flash.

Solutia trebuie sa poate simula atacuri phishing care redirectioneaza utilizatorii finali catre servere web continad continut malitios sau care servesc ca impersonatori ai traficului web legitim in ideea de a evalua posibilele pierderi de date.

Solutia trebuie sa aiba capabiltiatea de a efectua teste de phising fara a folosi statiile de lucru ale utilizatorilor finali.

Solutia trebuie sa ofere testerilor posibilitatea de a determina daca o statie de lucru o data compromisa expune si altea statii de lucru din aceeasi retea. Solutia trebuie sa permita ca statia compromisa sa fie folosita ca si cap de pod de unde sa se poata lansa atacuri aditionale impotriva retelei backend.

Teste pentru securitatea retelelor wireless

Solutia trebuie sa include capabilitati privind descoperirea si analizarea retelelor wireless, atat a punctelor din retea autorizate cat si a celor neautorizate.

Solutia trebuie sa poata evalua siguranta retelelor criptate cu WEP, WPA si WPA-2.

Solutia trebuie sa poata replica atacurile de tip “ man in the middle” in cazul retelelor wireless.

Solutia trebuie sa poate detecta sisteme ce executa cautari pentru SSID-uri.

Solutia trebuie sa fie capabila sa emuleze SSID-uri, prin care utilizatorul sa poata face:

- Marcarea masinilor conectate
- Incercarea de a ataca respective maisna la nivel de infrastructura
- Incercarea de colectare a credentialelor
- Inserarea de exploit-uri in traficul maisnilor conectate
- Influentarea traficului utilizatorului acelei statii de lucru
- Executia oricaror teste disponibile in partea de atac al retelei puse la dispozitie de solutie

Raportare

Solutia software trebuie sa ofere capabilitati de raportare.

Raportele solutiei trebuie sa includa standardele industriale privind evaluarile de risc:

- Numere CVE: Common Vulnerabilities and Exposures (CVE). Sunt identificatori publici pentru vulnerabiltiatile cunoscute
- Scoruri CVSS: The Common Vulnerability Scoring System (CVSS) - reprezinta un standard universal de evaluare a severitatii vulnerabilitatilor cunoscute.
- CPE: Common Platform Enumeration (CPE). Este o schema structurata de numire a sistemelor IT, platformelor si pachetelor.

Se doresc cel putin urmatoarele rapoarte:

- Raport ce include o reprezentarea vizuala a felului in care testele pot folosi vulnerabilitati individuale si a felului incare ele pot obtine acces la alte sisteme si aplicatii.
- Raport ce afiseaza rezultatele testelor necesare urmaririi alinierii la standarul de securitate ale datelor PCI (Payment Card Industry).
- Raport ce afiseaza rezultatele testelor effectuate de entitati guvernamentale necesare urmaririi alininerii la standardul FISMA (Federal Information Security Management Act of 2002).
- Raport ce sintetizeaza o arie larga de teste diverse necesare pentru a da companiei o viziune completa a vulnerabilitatilor existente atit la nivelul diverselor echipamente cat si la nivelul statiilor de lucru.
- Raport de trend, pentru a putea urmari datele rezultate din maxim 52 de teste de-a lungul timpului, repezentari grafice ale schimbarilor in postura de securitate a orgnizatiei pe masura ce vulnerabilitatile sunt identificate, remediate si retestate.
- Raport ce ofera informatii despre fiecare bresa de securitate care ar putea fi folosita in timpul testarii. Include pe cele disponibile in cazurile de atac de tip SQL Injection, Cross-Site Scripting and Remote File Inclusion.
- Raport ce ofera informatie in mod sumarizat in legatura cu fiecare pagina de web vulnerabila gasita in cadrul testelor si cum s-ar putea fi exploatata acea vulnerabilitate de un eventual atacator.
- Raport de activitate ce ofera un log detaliat al activitatilor de testing care se desfasoara incluzand datele relevante pe care comania le poate oferi auditorilor care revizuiesc programul de securitate al acesteia.

- Raport ce ofera un nivel ridicat de vizibilitate, al totalitatii testelor demonstrand ce vulnerabilitati exista, unde sunt localizate, cum pot fi folosite, si de unde poate incepe activitatea de remedire.
- Raport ce ofera utilizatorilor detalii precise privind cum pot fi compromise sistemele si aplicatiile lor atat de catre atacuri din lumea reala cat si de activitatea malware-lui.
- Raport ce oferta utilizatorilor detalii specifice despre toate bresele folosite cu success in cadrul testarii si modul in care acele brese pot fi utilizate de catre atacatori pentru obitinerea controlului asupra unui system testat si folosirea sa ca si “cap de pod”pentru alte atacuri.
- Raport ce ofera rezultate detaliate despre evaluarile facute pe statiile de lucru si utilizatori finali incluzand informatii despre tacticile de social engineering utilizate pentru activarea testelor.
- Raport ce ajuta companiile sa evalueze nivelul de pregatire al utilizatorilor finali vis a vis de atacurile bazate pe tehnici de social engineering .
- Raport ce detaliaza retelele wireless descoperite, cum se face relationarea client-AP si informatii despre profilul AP –ului. De asemenea mai contine informatii despre retele testate, care a fost gradul de compromitere si ce vulnerabilitati au dus la aceasta.
- Raport ce inmagazineaza informatii despre toate echipamentele mobile accesate in cadrul testelor.

4.5.2.4.3 Solutie mobila pentru investigaţii de tip FORENSIC

Soluţia trebuie să includă capabilităţi pentru efectuarea de investigaţii de tip FORENSIC in diferite locaţii fizice “on location” şi medii IT (reţele, PC-uri isolate, soluţii de stocare etc.).

Soluţia se constituie dintr-un echipament de calcul mobil de tip laptop şi un kit portabil de accesorii utile in procesul de colectare a probelor digitale.

Specificaţiile tehnice ale echipamentului de tip laptop sunt:

	Componenta	**Specificatii tehnice minimale si obligatorii**
A.	**Display**	Minim 15”, LED backlight , rezoluţie Full HD (1920x1080)
B.	**Procesor**	Tip: Intel Core i7, 4 nuclee Frecventa procesor : min 2.0 GHz Cache L3: min 6 MB
C.	**Memorie RAM**	Minim 8 GB, DDR3
D.	**Stocare**	Hard Disk SATA, viteza minim 7200 RPM, capacitate de stocare minim 500 GB
E.	**Procesare grafică**	Placă grafică dedicată, memorie dedicată minim 1 GB GDDR5

F.	**Unitate optica**	- BluRay Burner minim 6x, pentru discuri BD-R - DVD writer minim 8x, pentru discuri DVD±R
G.	**Conectivitate**	- 10/100/1000 Gigabit Ethernet - WLAN 802.11b/g/n - Bluetooth
H.	**Facilităţi integrate**	- Card reader 9-in-1 (MMC/RSMMC/MS/MS Pro/MS Duo/SD/Mini-SD/SDHC/SDXC) - Cameră video digitală, miim 2.0 Megapixel - Microfon incorporat - Tastatură iluminată
I.	**Interfete integrate (fara adaptori)**	- 1 x DVI-I - 1 x HDMI Port - 1 x Displayport - 1 x Headphone jack - 1 x Microphone jack - 1 x Line-In jack - 1 x S/PDIF output jack - 1 x RJ45 LAN jack - 1 x USB 2.0 - 3 x USB 3.0 - 1 x IEEE 1394a - 1 x E-SATA Port (USB 3.0 Combo)
J.	**Caracteristici de securitate**	- Cititor de amprente - Suport pentru incuietoare de tip Kensington Lock

K.	**Accesorii**	- Geanta de transport rigidizată - hard disk portabil minim 1TB cu interfata USB 3.0 - stick de memorie USB minim 32 GB cu interfata USB 3.0

Kit-ul portabil de accesorii va avea următoarele caracteristici:

- Va conţine o familie completă de dispozitive de tip „Write Blocker” pentru interfaţarea cu dispozitive de stocare IDE, SATA sau SAS, astfel:
- Adaptoare şi cabluri externe pentru conectarea de diferite dispozitive de stocare externe, astfel:
    - 1 x Cablu interfaţare IDE 8"
    - 1 x Cablu interfaţare IDE 2"
    - 1 x Cablu interfaţă SATA
    - 1 x Cablu interfaţă SCSI-3
    - 1 x Adaptor HDD 1.8"
    - 1 x Adaptor HDD 2.5"
    - 1 x Adaptor HDD ZIF
    - 1 x Adaptor MicroSATA
- Toate componentele kit-ului se vor livra intr-o cutie specială pentru depozitarea şi transportarea acestora.

Livrabile

- Echipament de calcul mobil de tip laptop;
- Kit portabil de accesorii.

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **130 de zile** de lucru pentru implementarea de solutii software sau configurarea de aplicatii software COTS (Commercial-Off-The-Shelf).

4.5.2.5 Integrarea modulelor si portalului web si testarea solutiei software dezvoltate(Sub-activitatea 6.5)

Aceasta activitate presupune integrarea modulelor ce compun platforma software si a portalului web existent, CERT-RO, in vederea testarii solutiei informatice pentru simularea diverselor tipuri de atacturi Cyber.

Integrarea modulelor solutiei software se va face in corelare cu informatiile gazduite de portalul web CERT-RO, privind:

- anunturi privind evenimente in domeniu;
- anunturi privind amenintari nou identificate pe plan national si international;
- cercetare si informare privind noutatile tehnologice in domeniu;
- realizarea, la cerere, de auditari si evaluari de securitate sau teste de penetrare;
- estimarea vulnerabilitatilor si punerea la dispozitie de situatii actualizate privind incercarile de intruziune si servicii de localizare a surselor atacurilor, pe baza informatiilor transmise de furnizorii de retele si servicii de comunicatii electronice;
- diseminarea informatiilor de securitate cibernetica.
- alerte si atentionari privind aparitia unor activitati premergatoare atacurilor;
- gestiunea incidentelor la nivel national, in cooperare cu celelalte echipe CERT;
- diseminarea rezultatelor investigatiilor incidentelor de securitate cibernetica, cu respectarea prevederilor acordurilor de cooperare incheiate cu partenerii CERT-RO

In cadrul acestei activitati, prestatorul se obliga sa compuna scenarii de testare pentru functionalitatile solutiei informatice care sa acopere capabilitatile tehnice ale solutiei in concordanta cu informatiile continute in portalul web CERT-RO.

Site prezentare proiect

Se doreste constructia unui website multi utilizator care sa permita pe de-o parte utilizatorilor inregistrati introducerea si managementul de informatii publice pentru o mai buna transparenta catre publicul larg si pe de alta parte utilizatorilor neautentificati, vizualizarea informatiilor generale legate de derularea proiectului.

Scopul urmărit este acela de a pune la dispozitita publicului informatia, prin intermediul unui site de prezentare, intr-un mod organizat si usor de navigat, transparent usor de mentinut de catre personalul desemnat.

Pentru a atinge acest scop ofertantii vor trebui sa asigure:

a) Crearea unui site web pentru pentru promovarea si diseminarea informațiilor privind proiectul ‘Sistemul National de Combatere a Criminalitatii Informatice „Cyber Crime”’ care va respecta cerintele autoritatii contractante prezentate in acest caiet de sarcini si care va fi livrat in termen de 10 zile lucratoare de la semnarea contractului.
b) Crearea unei identitati coerente si in ton cu mesajul transmis de catre autoritatea contractanta.

c) Realizarea unor modele functionale
d) Structurarea informatiei
e) Punerea la dispozitie a unui mod de gestionare a utilizatorilor si a drepturilor aferente acestora.
f) Implementarea unei baze de date cu format unitar.
g) Cumpararea si configurarea unui domeniu .ro pentru site-ul proiectului
h) Configurarea serverului pentru gazduire site
i) Optimizarea si promovarea paginilor web ale site-ului folosind tehnici de Search Engine Optimization (SEO).
j) Garanție – Dupa livrarea site-ului ofertantul va trebui să asigure garantie pe perioada implementării contractului, luând în calcul următoarele:
    - website-ul si bazele de date se vor afla pe serverul unui furnizor de hosting; se va prezenta contractul ofertantului cu furnizorul de hosting ;
    - pentru asigurarea mentenanţei, Prestatorul trebuie să opereze la o capacitate adaptată necesităţilor beneficiarului pe durata programului de lucru (cel puţin un om alocat conform unui interva orar agreat prin contract, în intervalul orar 8 – 18);
    - Prestatorul trebuie să asigure suport prin e-mail şi suport telefonic si să răspundă imediat la solicitările primite;
    - In cazul unor sesizări care presupun un timp mai îndelungat de răspuns, la propunerea Prestatorului, se va stabili un termen, cu acordul Beneficiarului;
    - Prestatorul va trebui să asigure suport tehnic pentru identificarea naturii disfuncţionalităţilor semnalate şi să declanşeze prompt procedurile specifice de remediere;
    - Prestatorul va asigura un backup zilnic al bazelor de date care vor fi gazduite pe serverul prestatorului; Lunar prestatorul va oferi beneficiarului un backup pe format fizic tip cd.
    - Prestatorul va trebui să asigure minim 1(una) persoană pentru serviciul de garantie
    - In perioada de garantie Prestatorul are obligatia de a remedia erorile de sistem raportate de catre utilizatori prin intermediul canalelor de comunicare.

Ofertanţii trebuie să însoțească în mod obligatoriu oferta tehnică de CD-uri, DVD-uri și/sau documente tipărite, prin care să dovedească că au capacitatea tehnică, creativă si informaţională de a realiza solicitările mai sus menționate. Acestea fac parte integrantă din propunerea tehnică iar neprezentarea lor atrage după sine eliminarea ofertei ca fiind neconformă.

Modul în care ofertantul intelege obiectivele stabilite de prezentul caiet de sarcini şi rezultatele asteptate:

- **Prezentarea de către ofertant a prototipurilor vizuale ce vor prezenta informatii considerate ca fiind esenţiale pentru obţinerea rezultatelor aşteptate ale contractului şi atingerea obiectivelor stabilite de acest caiet de sarcini.**

Prin prototip vizual intelegem varianta de prezentare grafica ce integreaza armonios chromatic, identitatea proiectului si informatiile prezente in site, aceasta varianta trebuie sa fie clar distincta din punct de vedere cromatic si al organizarii in pagina fata de alte variante propuse pentru acest proiect de acelasi candidat.

Prototipurile trebuie sa respecte sandardele W3 in vigoare si sa inglobeze principii de User Experience cu scopul de a facilita navigarea.

Ofertantii vor prezenta minim 3 versiuni de prototip vizual.

- **Prezentarea de către ofertant a modelelor de organizare a informatiilor considerate ca fiind esenţiale pentru obţinerea rezultatelor aşteptate ale contractului şi atingerea obiectivelor stabilite de acest caiet de sarcini.**

Modelul de organizare al informatiilor este o modalitate de aranjare in pagina a informatiilor pentru parcurgerea facila a acestora de diversele categorii de public vizat, acestea trebuie sa fie unice ca si prezentare si argumentate clar si obiectiv.

Ofertantii vor prezenta minim 2 versiuni de modele de organizare.

Ofertantul va descrie resursele de timp, cele umane si pe cele materiale, pe care acesta le va folosi pentru finalizarea cu succes a acontractului si pentru acoperirea tuturor cerintelor beneficiarului.

Ofertantul va trebui sa asigure gazduirea site-ului pentru toata durata proiectului pe un server care sa asigure urmatoarele cerinte minime si obligatorii:

- Sa suporte un numar de minim 100 utilizatori concurenti
- Up-time-ul serverului va fi de minim 99,9% pe toata perioada de hostare
- Serviciul de mententanta tehnica asociat gazduirii site-ului trebuie sa fie de 24 ore pe zi
- Serverul trebuie sa permita un trafic lunar optim si o capacitate adaptată necesităţilor beneficiarului, minim 100GB lunar.
- Asociate domeniului site-ului vor fi cel putin 20 de adrese de e-mail configurate si mentinute de catre prestator.

Cerinte tehnice generale si specifice

Ofertantul trebuie sa prezinte in oferta tehnica raspuns pentru urmatoarele cerinte generale considerate de catre autoritatea contractanta ca fiind minime si obligatorii.

Cerințe tehnice generale:

- Site-ul va trebui să fie flexibil, relativ simplu de modificat şi configurat în timp;
- Site-ul va oferi un design modern, plăcut, ergonomic, funcţional dar simplu de utilizat la nivelul interfeţei cu utilizatorul;
- Interfețele vor fi proiectate astfel încât să fie utilizate optim la o rezoluţie de minim 1024x768;
- Site-ul trebuie să poată fi utilizat cu precădere folosind mouse-ul (navigare, selectare în meniuri, manipulare controale, etc) şi tastatura (introducere date);
- Toate paginile site-ului vor avea o structurara asemanatoare de continut fapt care va facilita navigarea in site, vizualizarea informatiilor, gestionarea acestora intr-o maniera simpla si eficienta.
- Actualizarea datelor şi accesul la acestea din sistem se vor realiza în timp real, printr-o interfață de administrare ușor accesibilă pentru utilizatori și protejată prin parolă;
- Toate functionalitatile site-ului trebuie sa fie accesibile printr-un browser web. Tehnologiile folosite in dezvoltare trebuie sa fie deschise şi neproprietare
- Baza de date a site-ului trebuie sa lase posibilitatea de a fi integrata cu alte sisteme informatice.
- Structura propusa trebuie să fie astfel construita incat sa permita dezvoltări ulterioare si integrări cu alte sisteme cu un efort mic;
- Este necesar ca sistemul sa suporte diacritice;
- Comunicaţia dintre server și client trebuie să fie securizata;
- Accesarea modulului de administrare sa se faca securizat pe profile de utilizator;
- Site-ul va fi optimizat pentru cel putin trei browsere (IE, Mozilla, Chrome) , dintre cele mai utilizate pe piata romaneasca.
- Site-ul va fi optimizat pentru motoarele de cautare prin tehnici specifice SEO
- Personalul autoritatii contractante responsabile de utilizarea site-ului va fi instruit pentru realizarea următoarelor activităţi: instalare, configurare, utilizare, menţinere şi modificare a informatiilor din sistem;
- Codul sursa rezultat in urma dezvoltarii va fi proprietatea beneficiarului.
- Pentru asigurarea compatibilității site-ului cu soluțiile déjà existente la beneficiar, se vor folosi tehnologii de dezvoltare opn-source (PHP, Apache, MySQL, AJAX).

Ofertantul trebuie sa prezinte in oferta tehnica raspuns pentru urmatoarele cerinte specifice considerate de catre autoritatea contractanta ca fiind minime si obligatorii.

Cerințe specifice:

1. Site-ul trebuie sa permita administrarea utilizatorilor si a autorizariilor de acces a acestora;
2. Crearea unei structuri de utilizatori cu drept de scriere, publicare sau citire a informatiilor cu forma:
    - Recenzor: Utilizator cu drept de creare, stergere, arhivare si publicare a materialelor generate pe site-ul realizat.
    - Editor: Utilizator cu drept de creare, stergere si arhivare de continut pe site-ul realizat.
    - Cititor: Orice vizitator care poate naviga paginile publice ale site-ului.
3. Accesul in sistem se va realiza doar folosind cont de utilizator si parola;
4. Utilizatorii trebuie sa-si poata modifica datele personale si parola;
5. Administratorul trebuie sa poata monitoriza performanta sistemului si istoricul de activitate al utilizatorilor;
6. Prestatorul va pune la dispozitia Beneficiarului un modul de administrate tip „WYSIWYG” modul care permite editarea continutului identic cu ceea ce apare in interfata utilizator.
7. Sistemul trebuie sa includa posibilitatea vizualizarii de rapoarte statistice privind utilizarea site-ului la nivel national cat si la nivel international;
8. Pe prima pagina a site-ului trebuie sa fie afisata, structura de informatii, informatiile despre proiect, identitatea proiectului, stiri de ultima ora, modul de cautare in site, un mod de inregistrare sau autentificare a membrilor utilizatorilor, cu utilizator si parola.
9. Intre sectiunile din site trebuie sa existe o sectiune in care sa se prezinte obiectivele specifice ale proiectului.
10. O alta sectiune trebuie sa contina o lista cu activitatile propuse, rezultate anticipate.
11. Site-ul trebuie sa contina prezentarea grupului tinta la care ne raportam.
12. Site-ul va contine un forum cu inregistrare in care se va face comunicarea cu grupul tinta si partenerii din proiect
13. Site-ul va contine o sectiune de contact, cu datele de contact ale beneficiarului.
14. Înainte de realizarea recepției site-ul, alături de celelalte componente ce vor asigura accesul public la acesta (ex: server web, server BD, certificate digitale etc.) va fi evaluat dpdv al securității de către beneficiar. Orice vulnerabilitate identificată (ex: SQLi, XSS, vulnerabilități ale serverului web) va trebui remediată de ofertant înainte de realizarea recepției.

Livrabile

- Document cu scenarii de testare;
- Raport de testare;
- Site de prezentare proiect

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **60 de zile** de lucru.

4.5.2.6 Instruire Utilizatori si administratori sistem (Sub-activitatea 6.6)

Prestatorul trebuie sa ofere servicii profesionale de instruire pentru toate componentele soluției informatice livrate (platformă hardware de bază, soluție integrată de virtualizare, software securitate de bază, soluție software pentru simularea atacurilor cyber, soluție mobilă de testare precum și pentru toate celelalte componente hardware sau software livrate). Astfel, prestatorul va organiza la livrarea solutiei, sesiuni de instruire pentru buna intelegere a functionarii solutiei si a modului de utilizare. Sesiunile de instruire se adreseaza utilizatorilor solutiei informatice si administratorilor de sistem și vor acoperi toate echipamentele și pachetele software livrate. Acolo unde producătorul soluției livrate permite, vor fi livrate cursuri de certificare a administratorilor și a utilizatorilor soluției.

Activitatea de instruire vizează instruirea și certificarea unui număr de **9 persoane** (3 administratori de sistem și 6 utilizatori ai soluției).

Instruirea trebuie facuta de către experți/traineri certificați pe fiecare soluție în parte. Prestatorul se obliga sa faca dovada certificarii trainerilor.

Livrabile

- Cel putin 9 de persoane instruite si certificate pentru administrarea și utilizarea soluțiilor informatice livrate.
- Utilizatorii solutiei informatice instruiti si actualizati cu modul de lucru cu platforma informatica oferita;
- Prezentare (slide-uri) pentru instruirea utilizatorilor platformei software cu detaliere functionalitati si mod de lucru pentru fiecare modul;
- Manuale de utilizare pentru solutiile software și hardware livrate;

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **20 de zile** de lucru.

4.5.2.7 Cerinte privind sustenabilitatea sistemului

Perioada de licențiere a tuturor sistemelor/componentelor (software) tip „commercially available off-the-shelf" incluse în oferta trebuie să fie de minim 12 luni de la data recepției sistemului (aferenta LABORATORULUI DE TESTARE), data validata prin semnarea procesului verbal de recepție.

Serviciile de garanţie oferite vor include minim următoarele:

- Diagnosticarea, izolarea şi remedierea defectelor software semnalate de către Beneficiar;

- Suport software pentru defectele software semnalate ofertantului câștigător;
- Asistență cu instalarea de actualizări şi noi versiuni de programe puse la dispoziție de către producătorii de software tip COTS;
- Asistenta acordata Beneficiarului pentru aplicarea corecțiilor ca urmare a remedierii defectelor semnalate.

Ofertanții vor descrie în oferte planul detaliat privind garanția pentru implementarea software și produsele software livrate în cadrul proiectului.

Perioada de garanție pentru toate configurările si dezvoltările din cadrul sistemelor/componentelor software incluse în ofertă trebuie sa fie de 12 luni de la data de acceptanță a LABORATORULUI DE TESTARE.

Ofertanții vor descrie in oferta planul detaliat privind serviciile de garanție pentru configurările si dezvoltările software asigurate in cadrul proiectului/LABORATORULUI DE TESTARE.

***Perioada de garanţie pentru servere, switchuri fibre channel, swithcuri retea, echipament integrat de protectie a retelei, solutie profesionala de alimentare, echipament stocare, laptopuri* oferite trebuie să fie de minim 36 de luni de la data recepției sistemului (aferenta LABORATORULUI DE TESTARE), data validata prin semnarea procesului verbal de recepție.**

Garanţia pentru componentele hardware din cadrul proiectului, oferită la fata locului trebuie să fie disponibilă în toate zilele lucrătoare (8x5). Ofertantul câștigător va trebui să se prezinte la fata locului pentru constatarea defecțiunii în maxim 4 ore de la semnalarea acesteia de către Beneficiar, diagnosticarea defecțiunii se va face în maxim 8 ore de la constatarea acesteia, iar înlocuirea sau repararea componentelor hardware defecte se va face în decurs de 15 zile lucratoare de la diagnosticarea defecțiunii. În situaţia în care este necesară preluarea echipamentelor de către furnizor pentru reparaţii sau înlocuire, unităţile de stocare vor rămâne la beneficiar.

Ofertanții vor descrie în oferte planul detaliat privind garanţia hardware asigurată în cadrul proiectului.

Echipamentele ofertate şi livrate NU TREBUIE SĂ FIE clasificate în cadrul categoriilor ”End of Life” şi nici ”End of Sales”.

Garanția privind sistemul informatic din cadrul proiectului trebuie să fie disponibilă în toate zilele lucrătoare (8x5) şi trebuie să garanteze remedierea defectelor hardware și software semnalate de Beneficiar conform următorului tabel de gravitate (SLA):

Nivel de Gravitate	Descriere	Reacție inițiala a Ofertantului câștigător (ore)	Timp total de diagnosticare a defectului software (zile lucrătoare)
1	Defect major, sistemul nu este funcţional	4	8
2	Defect mediu, unele funcţii sau componente ale sistemului nu sunt funcţionale	4	16

3	Defect minor, unele funcţii sau componente ale sistemului sunt afectate dar funcţionale	4	24

4.5.2.8 Note finale

Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse, aceste specificatii vor fi considerate ca avand mentiunea sau echivalent.

4.5.3 Definirea unui set de politici publice, propuneri de acte normative, proceduri in vederea combaterii criminalitatii informatice (Activitatea 7 a proiectului)

Combaterea si investigarea infractiunilor informatice comporta atat o latura tehnico-stiintifica determinata de metodologii si tehnici de investigare utilizate in vederea obtinerii probelor digitale, cat si la o latura juridica caracterizata de legislatia in vigoare privind criminalitatea informatica. Pentru o mai buna intelegere a fenomenului de criminalitate informatica, este necesara o analiza a legislatiei interne si internationale in domeniul criminalitatii informatice, avand in vedere in special cooperarea internationala si europeana in domeniul combaterii criminalitatii informatice, daca se ia in calcul caracterul transfrontalier al tipului de infractiuni informatice.

La nivel international exista organizatii care au analizat in mod constant dezvoltarea fenomenului criminalitatii informatice si care au creat strategii de prevenire si combatere a acestui fenomen. Principalele organizatii internationale implicate in studiul fenomenului de criminalitate informatica sunt urmatoarele: Consiliul Europei, Organizatia Natiunilor Unite, Grupul G8, Uniunea Internationala a Telecomunicatiilor si Interpol-ul. In plus fata de organizatiile internationale, care actioneaza la nivel global, exista si organizatii regionale care sunt concentrate pe anumite zone in rezolvarea problemelor de criminalitate informatica: Uniunea Europeana, Organizatia pentru Cooperare si Dezvoltare Economica, Grupul APEC, Commonwealth, Liga Araba si Consiliul de Cooperare din Golf, Organizatia Statelor Americane. Majoritatea analizelor realizate de grupurile de lucru consituite de expertii din cadrul institutiilor enumerate au stat la baza punerii pilonilor legislativi in domeniul politicilor publice, actelor normative si procedurilor dezvoltate in vederea prevenirii combaterii criminalitatii informatice.

Prestatorul va defini un set de politici publice, propuneri de acte normative si proceduri, aliniate ultimelor standarde si tendinte in domeniu, usor aplicabile participantilor la traficul on-line din Romania.

4.5.3.1 Activitati de analiza, documentare, suport, in vederea formularii propunerilor de strategii, proceduri si acte normative (Sub-activitatea 7.1)

Cerinte generale

Prestatorul va elabora o analiza a politicilor publice si a bunelor practici de la nivelul Uniunii Europene in domeniul securitatii cibernetice, pe baza documentarii exhaustive, corecte si corelate a documentatiei existente in surse publice astfel incat analiza sa fie realizata pe baza unui spectru cat mai larg de informatii si optiuni.

Prestatorul va analiza si documenta cadrul general privind infractiunile informatice in sistemul juridic romanesc, modalitatea de reglementare a infractiunilor informatice reprezentata in Conventia Consiliului Europei privind criminalitatea informatica, precum si aspecte de drept comparat privind criminalitatea informatica. Analiza si documentarea va avea ca surse de cercetare interna, cadrul penal national privind infractiunile informatice precum si studiile de practica judiciara strategii si proceduri de la nivelul IGPR, PICCJ, INM iar ca surse externe studiile, bunele practici si elemente de politici publice de la nivelul a cel putin doua organisme europene specifice.

Documentarea la sursele mentionate va avea ca obiect de timp perioada anilor 2010, 2011 si 2012.

Cerinte specifice

In Romania, cea mai importanta reglementare juridica aplicabila in acest moment in domeniul criminalitatii cibernetice este Legea nr.161/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei. Aceasta lege prezinta principalele probleme legate de criminalitatea informatica si introduce un numar de opt infractiuni, care corespund clasificarilor si definitiilor prezentate in cuprinsul Conventiei Consiliului Europei privind criminalitatea informatica.

Legea nr.161/2003 reprezinta o buna adaptare a sistemului juridic romanesc la prevederile Conventiei Consiliului Europei privind criminalitatea informatica, prin alinierea unor notiuni si termene precum: infractiunea de acces ilegal la un sistem informatic, infractiunea de interceptare

ilegala a unei transmisii de date informatice, infractiunea de alterare a integritatii datelor informatice, infractiunea de perturbare a functionarii sistemelor informatice, infractiunea de a realiza operatiuni ilegale cu dispozitive sau programe informatice, infractiunea de fals informatic, infractiunea de frauda informatica, la continutul si dispozitiile Conventiei.

Conventia Consiliului Europei privind criminalitatea informatica reprezinta cea mai importanta reglementare juridica internationala in domeniul criminalitatii informatice, deoarece aceasta tinde sa devina un instrument juridic global, fiind semnata si ratificata de un numar din ce in ce mai mare de state din intreaga lume. Aceasta Conventie isi propune sa previna actele indreptate impotriva confidentialitatii, integritatii si disponibilitatii sistemelor informatice, a retelelor, a datelor, precum si a utilizarii frauduloase a unor asemenea conduite si prin incurajarea adoptarii unor masuri de natura a permite combaterea eficace a acestor tipuri de infractiuni, menite sa faciliteze descoperirea, investigarea si urmarirea penala a acestora atat la nivel national, cat si international, precum si prin prevederea unor dispozitii materiale necesare asigurarii unei cooperari internationale rapide si sigure.

In vederea acoperirii unei arii exhausitive de studiu a punctelor de impact in zona securitatii cibernetice, se vor alcatui echipe mixte de lucru de experti calificati, pe urmatoarele arii de competenta:

- o echipă interdisciplinară, formată din 16 experți tehnici – în domeniul IT, ce va fi responsabilă de activitatile de analiza, documentare si furnizarea de cunostinte tehnice membrilor celorlalte echipe implicate in implementarea proiectului;
- o echipă formată din 4 experți în legislație si politici publice, care va trebui să furnizeze informații cu privire la aspectele legislative naționale și internaționale în vigoare referitoare la prevenirea și combaterea criminalității informatice;

Selectionarea membrilor celor două echipe va fi realizată cu consultarea și cu avizul beneficiarului.

Aceste echipe vor constitui baza de lucru pentru îndeplinirea obiectivului strategic al proiectului. În acest sens, diseminarea și optimizarea rezultatelor activității desfășurate de grupul de experți se va efectua prin organizarea a 5 evenimente de tip „ateliere de lucru”, între reprezentanți ai companiilor IT&C, administrației publice, mediul educațional, experți din cadrul proiectului și experți externi.

Recomandarile privind provenienta expertilor tehnici din cadrul echipelor descrise mai sus vor cuprinde urmatorul spectru de tipuri de profil, astfel incat sa fie acoperite toate zonele de compententa necesare indeplinirii activitatii:

- profesori / cadre universitare cu experienta in zona domeniului juridic/ securitatii cibernetice;
- magistrați cu experiență în domeniu;
- membri in cadrul unor organizatii nonguvernamentale cu expertiza si arie de activitate in domeniul securitatii cibernetice;
- experti din cadrul institutiilor de stat ce au atributii in domeniul securitatii cibernetice;
- experti in activitati de ethical hacking;

Livrabile

- Un set de documente suport care sa cuprinda totalitatea activitatii de analiza si documentare (intalniri, ateliere de lucru, analize de impact, conferinte, consultari, etc.) in vederea formularii propunerilor de strategii, proceduri si acte normative;
- Document suport privitor la calificarea fiecarei chestiuni analizate, din punct de vedere al naturii juridice, in vederea identificarii cadrului legislativ specific in a carui raza de reglementare se va subsuma.

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **1200 de zile** de lucru.

4.5.3.2 Elaborarea documentelor de politici publice rezultate in urma studiilor,analizelor si dezbaterilor (Sub-activitatea 7.2)

Introducere

Principalele institutii cu caracter national care au rol in prevenirea si/sau combaterea infractiunilor informatice sunt organisme cu ramificatii guvernamentale precum cele din subordinea Politiei Romane, respectiv Directia de Combatere a Crimei Organizate si institutul de Criminalistica, dar si alte institutii precum Directia de Investigare a Infractiunilor de Criminalitate Organizata si Terorism, precum si structuri din cadrul serviciilor de informatii.

In elaborarea documentelor de politici publice in urma studiilor, analizelor si dezbaterilor realizate cu toti actorii implicati pe scena locala, prestatorul va trebui sa tina cont de totalitatea actelor normative emise sau aflate in lucru pana la data prestarii in materia criminalitatii informatice, de tendintele si prevederile principalelor reglementari de la nivelul organismelor Uniunii Europene (atat surse institutionale, cat si organisme private cu reputatie in domeniu), dar si de principalele atributii ale institutiilor nationale responsabile in lupta de prevenire, combatere si aplicare de pedepse in domeniul savarsirii de infractiuni informatice.

Cerinte generale

Prestatorul va elabora propuneri de politici publice in domeniul combaterii fenomenului de criminalitate informatica, politici care se vor putea materializa in actiuni concrete in plan legislativ, tehnic si de preventie.

Cerinte specifice

In cadrul acestei activitati vor trebui identificate si elaborate propuneri pentru completarea politicilor publice in domeniul prevenirii si combaterii criminalitatii informatice pe teritoriul Romaniei, politici care vor trebui armonizate cu cadrul normativ european, avand in vedere caracterul transfrontalier al infractiunilor informatice.

Astfel, prestatorul va defini un set de politici publice, avand minim urmatorii parametrii:

- obiectivele urmarite prin implementarea masurilor propuse;
- grupul/grupurile tinta, arii si domeniile vizate;
- actorii implicati (stakeholder-i) in aprobarea si implementarea masurilor;
- durata estimata de implementare;
- aria geografica de impact;
- costul / resursele necesare implementarii politicii publice pe un termen de 5 ani;

Prestatorul va defini un set de politici publice recomandate a fi implementate.

Referitor la definirea setului de politici publice, propuneri de acte normative si proceduri in materia metodelor de combatere a criminalitatii cibernetice, acestea trbuie sa aiba ca obiective principale cel putin urmatoarele directii de actiune (fara a se limita la):

- Analiza legislatiei din domeniul de referinta;
- Elaborarea de propuneri legislative si de solutii care sa permita protectia spatiului cibernetic si a utilizatorilor acestuia.
- Identificarea, analiza si optimizarea platformelor existente, identificarea unor solutii legislative si metodologice de consolidare a lor la nivel national;
- Analiza si identificarea oportunitatilor de realizare a unui sistem de semnalare a tuturor incidentelor relationate criminalitatii cibernetice
- Stabilirea unor criterii si metode care sa conduca la imbunatatirea managementului riscurilor globale in spatiul virtual;

Prestatorul va evalua politicile publice propuse in raport cu cel putin urmatoarele criterii:

- Relevanta obiectivelor propuse fata de planul de dezvoltare si recomandarile din *Activitatea 5*;

- Gradul de armonizare si aderare a masurii la bunele practici din domeniu si la standardele Uniunii Europene – masurile cele mai importante in vederea aderarii la standardele internationale si UE;

- Fezabilitatea metodologiei de implementare propuse:
    - Gradul de impact– masurat ca marimea grupului tinta, ariilor si a domeniilor afectate de masura respectiva;
    - Analiza cost-beneficiu – masurile cele mai bine pozitionate la capitolul beneficii versus cost;
    - Sustenabilitatea – masura este sau nu sustenabila pe o perioada de minim 5 ani;
    - Usurinta de implementare – masuri imediate.

Livrabile

- Un set de politici publice necesare a fi implementate;
- Document suport de identificare a ariei legislative careia se subsumeaza fiecare politica publica necesar de implementat;
- Elaborarea unui set de documente suport cuprinzind: propuneri de acte normative;

Volumul de lucru

Pentru realizarea acestei activitati, Prestatorul va aloca un numar de **800 de zile** de lucru.

4.5.4 Instruirea membrilor echipei CyberCrime şi a Secretariatului Permanent (Sub-activitatea 8.4 a proiectului)

In cadrul acestei activitati, un numar de **40 de persoane**, membri ai echipei Cyber Crime, constituite in cadrul proiectului, vor participa la diferite cursuri in vederea instruirii in materie de solutii de contracarare a criminalitatii cibernetice. Sesiunile de instruire se vor finaliza cu certificate de absolvire.

Ofertantul trebuie sa respecte cu strictete prevederile privind asigurarea suportului logistic, precum si sa depuna toate eforturile pentru indeplinirea tuturor cerintelor logistice aparute in implementarea proiectului, pentru fiecare sesiune de instruire / vizita pentru schimb de bune practici organizata in cadrul prezentului contract. Toate modulele de pregătire trebuie realizate astfel încât să permită utilizarea de către cursanți a platformei tehnice, achiziționate în cadrul proiectului, și implementate în LABORATORUL DE TESTARE.

Toate cheltuielile aferente derulării sub-activității 8.4 a proiectului vor fi realizate din bugetul alocat cheltuielilor conexe, în conformitate cu prevederile prezentului caiet de sarcini (pct. 7.3 Cheltuieli conexe)

Prestatorul va oferi servicii de pregătire a personalului, sub formă de module, care să respecte următoarele cerințe:

Modulul I – Curs specific ce va trata aspecte de ordin juridic și/sau politici publice cu referire la securitatea cibernetică (TRANSITS I sau echivalent).

Obiectivul acestui modul este însușirea de către participanții la programul de pregătire ”Cyber Crime” a unui volum suficient de cunoştinţe teoretice pe baza cărora aceştia să poată contribui la îmbunătăţirea sistemului de management al securităţii informaţiilor şi la constituirea şi operaţionalizării unor echipe sau structuri de tip CERT, în instituţiile de unde provin.

Pentru îndeplinirea obiectivului, cursul trebuie să prezinte elementele şi noţiunile de bază privind securitatea cibernetică, combaterea criminalităţii informatice, organizarea şi funcţionarea structurilor de tip CERT şi rolul acestora în managementul incidentelor de securitate cibernetică.

Programa cursului va include teme prin care să se acopere următoarele aspecte:

- cadrul general de reglementare şi conceptele utilizate la nivel internaţional şi naţional în domeniul securităţii cibernetice;
- cadrul legal privind prevenirea, combaterea şi incriminarea faptelor de criminalitate informatică;
    - aspecte privind incriminarea infracțiunilor informatice, incidente în domeniul securității cibernetice.
    - aspecte de ordin procedural privind investigarea infracțiunilor informatice (noțiunea de probe, mijloace de probă specifice, colectarea și conservarea probelor ș.a).
- proceduri/reglementări interne/internaționale în referire la domeniul securității cibernetice privind:
    - aspecte ce pot afecta echipele de răspuns la incidente de securitate cibernetică din România și Uniunea Europeană, NATO şi procedurile operative cu care ar trebui să fie familiarizate echipele de acest tip (noţiuni de protecţia datelor, utilizarea incorectă a sistemelor informatice, monitorizarea reţelelor, colectarea probelor digitale şi colaborarea cu organele de cercetare ș.a).

- organizarea echipelor de răspuns la incidente de securitate cibernetică, de tip CERT din România, Uniunea Europeană și NATO: planificare, definirea constituenţei, prezentarea serviciilor oferite şi metodele de comunicare cu alte entităţi.
    - responsabilitățile și procedurile de lucru ale unităților de tip CERT;
    - procedurile și modalitățile de lucru ale instituțiilor responsabile cu investigarea incidentelor de securitate și a atacurilor cibernetice;
- gestionarea incidentelor: procesul de gestionare a incidentelor de securitate cibernetică plecând de la raportul iniţial despre incident, continuând cu trierea, investigarea, rezolvarea, închiderea/clasarea şi analiză ulterioară;
    - modele organizatorice privind managementul riscurilor de securitate cibernetică şi managementul incidentelor de securitate cibernetică;

- Durata cursului va fi de 5 zile – 8 ore pe zi.
- Se vor sustine doua sesiuni de pregatire pentru un numar de **40 cursanți** organizați în două grupe a câte 20 de persoane.

Modulul II – Curs de tip ”ethical hacking”, ”penetration test” sau echivalent

Scopul acestui modul de pregătire este să transfere membrilor echipei CYBERCRIME, cunoștințe cu privire la tipuri de incidente, tehnici și procedee de detecţie a evenimentelor asociate incidentelor de securitate la nivelul infrastructurii TIC, prin care să poată asigura un răspuns coordonat, eficient și rapid în situația detectării unor atacuri informatice adresate către sisteme informatice.

La finalizarea stagiului de pregătire cursanții trebuie să dețină cunoștințele referitoare la metode și tehnici de penetrare a securității sistemelor informatice precum și tehnici de prevenire și contracarare pentru, cel puțin, următoarelor tipuri de atacuri informatice:

- scanarea rețelelor informatice și identificarea resurselor active (footprinting, reconaissance, scanning etc.)
- identificarea și exploatarea vulnerabilităților;
- interceptare și monitorizare trafic rețea (MITM)
- social engineering
- DoS/DDoS
- atacuri asupra serverelor și serviciilor web

- atacuri asupra serverelor de baze de date (SQLi)
- atacuri asupra aplicațiilor web (ex: XSS etc.)
- atacuri de tip code injection și buffer overflow
- atacuri asupra browserelor web
- testarea securității parolelor
- atacuri asupra rețelelor wireless
- tehnici de obstrucționare și eludare a echipamentelor de securitate de tip IDS, firewall, honeypot

Cerințe specifice: În cadrul cursului trebuie folosite soluțiile tehnice achiziționate în cadrul proiectului, respectiv din cadrul LABORATORULUI DE TESTARE, în special componentele soluției software pentru simularea atacurilor cyber. Cursul trebuie să fie dedicat activităților de penetration testing sau ethical hacker, să dureze minim **5 zile**, să fie recunoscut la nivel internațional, să se finalizeze cu examen de certificare. Cursul trebuie să fie susținut de un instructor autorizat/acreditat de către compania detinatoare a dreptului de organizare a cursului și susținut în cadrul unui centru de training autorizat. Prestatorul trebuie să asigure sala, toate echipamentele și materialele necesare desfășurării cursului. Cursul se va organiza pentru **20 de persoane in serii de maxim 10 persoane**. Predarea se poate face în limba română sau în limba engleză.

MODULUL III: CURS DE INVESTIGAȚII DIGITALE DE TIP FORENSIC ȘI ANALIZĂ MALWARE

A. INVESTIGAȚII DIGITALE DE TIP FORENSIC

Scopul acestei componente a cursului este transferarea către membri echipei Cyber Crime de cunoştinţe şi abilităţi pentru desfăşurarea de analize şi investigaţii (digital forensic) ori activități specifice cercetării penale asupra probelor digitale pentru a identifica natura incidentului sau a infracţiunii informatice, autorul sau atacatorul, scopul, mecanisme de atac utilizate, modalități de desfăşurare, vulnerabilităţi exploatate, împrejurări care au favorizat producerea evenimentului, impactul şi prejudiciile produse, asigurarea integrității și disponibilității sistemelor informatice, folosirea aplicațiilor de tip forensic în analiza sistemelor informatice si a dispozitivelor de stocare, inclusiv smartphone și tablete, analiza și cercetarea sistemelor sau rețelelor informatice în timpul funcționării acestora, analiza malware, investigații prin folosirea resurselor oferite prin Internet.

La finalizarea stagiului de pregătire cursanții trebuie să dețină cunoștințele referitoare la investigații digitale de tip forensic, pentru cel puțin următoarele domenii:

- analiza și cercetarea în timp real a sistemelor sau rețelelor informatice
- colectare și analiza probe digitale
- recuperare fișiere de pe diferite tipuri de sisteme de stocare și din formate diferite.
- utilizarea diferitelor instrumente de tip forensic (ENCASE, AccessData FTK etc.)

- corelare loguri și evenimente de securitate
- investigare loguri, trafic rețea
- investigare atacuri wireless
- investigare atacuri asupra aplicațiilor sau serverelor web
- urmărire și investigare email-uri
- tehnici de investigare a echipamentelor mobile (telefoane, tablete etc.)
- realizare de rapoarte investigative
- tehnici specifice de investigare pentru Windows, Linux, Mac OS X.

Cerințe specifice: În cadrul cursului trebuie folosite soluțiile tehnice achiziționate în cadrul proiectului, respectiv din cadrul LABORATORULUI DE TESTARE, în special componentele soluției mobile pentru investigații de tip forensic. Componenta cursului trebuie să fie dedicată activităților de forensic, să dureze minim **5 zile (8 ore/zi)**, să fie recunoscută la nivel internațional, să se finalizeze cu examen de certificare. Predarea trebuie să fie susținută de instructori autorizați/acreditați, de către compania proprietară a dreptului de organizare a cursului, și să se desfășoare în cadrul unui centru de training autorizat. Prestatorul trebuie să asigure sala și toate echipamentele și materialele necesare desfășurării cursului. Predarea se poate face în limba română sau în limba engleză.

Componenta se va organiza pentru 20 de persoane in serii de maxim 10 persoane.

B. ANALIZĂ MALWARE

Componenta cursului trebuie să prezinte, cel puțin:

- IDA Pro scripting pentru automatizarea procesului de analiză statică
- analiză dinamică avansată prin utilizarea sistemelor de tip scriptable debuggers
- analiză aplicaţii compilate în diverse limbaje de programare (C**, .NET, Visual Basic, Delphi şi Perl2Exe)
- tehnici de despachetare şi reconstrucţie executabile
- evitarea tehnicilor anti-reverse engineering (detecţie maşini virtuale, detecţie debugger, detecţie HW BP şi SW BP, tehnici anti-dezasamblare)
- identificarea şi gestionarea tehnicilor de criptare/codare a datelor
- identificarea şi colectarea aplicaţiilor malware stealth
- tehnici de analiză shellcode şi exploit-uri

Componenta cursului trebuie să cuprindă exerciţii şi laboratoare în care să fie predate cel puţin următoarele:

- Utilizarea script-urilor pentru simplificarea şi automatizarea operaţiilor de dezasamblare şi debugging
- Identificarea metodelor de obfuscare a codului
- Familiarizarea cu diferite limbaje de programare (înţelegerea detaliată a codului compilat)
- Identificarea tehnicilor de ascundere folosite de aplicaţiile malware
- Identificarea tehnicilor anti-analiză
- Analiza unor mostre de malware avansat

Cerințe specifice: În cadrul cursului trebuie folosite soluțiile achiziționate în cadrul proiectului, respectiv din cadrul LABORATORULUI DE TESTARE, în special componentele soluției mobile pentru investigații de tip forensic. Cursul trebuie să fie dedicat activităților de analiză de malware și are o durată de minim 5 zile – 8 ore pe zi. Prestatorul trebuie să asigure sala, toate echipamentele și materialele necesare desfășurării cursului. Predarea se poate face în limba română sau în limba engleză.

Cursul se va organiza pentru 10 de persoane.

Modulul IV – curs specific de tip exercitiu cibernetic.

Modulul final va trebui să constituie un exercițiu de simulare a unui atac cibernetic la nivel național. Membrii echipei CYBERCRIME își vor demonstra abilitățile și cunoștințele deprinse în primele 3 module și vor contribui, din perspectiva instituțiilor din care fac parte, la rezolvarea rapidă și eficientă a crizei cibernetice simulate.

Astfel prestatorul, va trebui să dezvolte o serie de scenarii de atac, pe baza indicațiilor ulterioare furnizate de autoritatea contractantă, care să permită folosirea soluțiilor tehnice (din cadrul LABORATORULUI DE TESTARE) achiziționate în proiect, precum și a cunoștințelor dobândite de echipa CYBERCRIME.

Scenariile vor trebui să simuleze atacuri cibernetice la scară națională sau chiar internațională și să permită colaborarea experților și a instituțiilor din care aceștia provin, pentru remedierea rapidă a efectelor incidentului.

Exercițiul va fi organizat pentru 40 de persoane și va dura 3 zile.

Livrabile

- Cursurile pentru pregatirea membrilor echipei Cyber Crime.

Expertii contractati de catre prestator vor fi in prealabil avizati de catre beneficiar.

ATENTIE. Nerespectarea cerintelor privind activitatile si rezultatele descrise, inclusiv durata activitatilor, volumul de munca solicitat si livrabilele previzionate, vor conduce la considerarea ofertei ca fiind neconforma.

5 Management de proiect

Îndeplinirea obiectivelor proiectului înseamnă atingerea standardelor de calitate propuse, în limitele de timp şi de buget stabilite. Metodologia de management de proiect va pune la dispoziţie o serie de componente şi procese care să ajute în procesul de planificare, monitorizare şi control şi care să asigure că proiectul va fi realizat la timp, cu bugetul alocat, la nivelul de calitate programat şi cu atingerea tuturor obiectivelor propuse.

5.1 Cerinţe generale privind managementul implementării proiectului

Metodologia de management de proiect utilizată de Prestator va include următoarele componente:

- Organizarea proiectului.
- Planificarea proiectului.
- Controlul proiectului.
- Managementul riscurilor.
- Managementul calităţii.
- Managementul configuraţiilor.
- Controlul schimbării.

Astfel, din punct de vedere al organizării, proiectul va fi condus la nivel strategic de un Comitet de Conducere, care va stabili și controla direcția în care evoluează proiectul. Includerea în Comitetul de Conducere a unor persoane cu funcții de răspundere în cadrul instituțiilor de care aparțin va asigura atât respectarea intereselor tuturor celor afectați de proiect, cât și o alocare corespunzătoare a resurselor pe durata proiectului. Liderul de echipă al Prestatorului va raporta către echipa de management de proiect a beneficiarului (atât internă cât și externalizată), iar aceasta va raporta în mod periodic către Comitetul de Conducere al proiectului asupra evoluției proiectului. Prestatorul va sprijini această activitate de monitorizare prin furnizarea periodică (cel puțin lunară) a informațiilor relevante despre evoluția proiectului.

Monitorizarea și raportarea către echipa de management a beneficiarului va include cel puțin următoarele:

- sedințe bi-lunare pentru evaluarea progresului implementării, în cadrul cărora se vor discuta acțiunile finalizate, cele preconizate pentru perioada următoare, eventuale dependențe, probleme sau riscuri;
- rapoarte lunare de stare în care se vor descrie: activitățile planificate și finalizate, cele întârziate și motivul, activitățile preconizate pentru perioada de raportare următoare și dependențele pe care trebuie să le satisfacă beneficiarul, situația financiară a proiectului (situația la zi a bugetului proiectului) și graficul de implementare actualizat al proiectului ("tracking Gantt")
- prezentarea stadiului proiectului în cadrul ședințelor Comitetului de Conducere al proiectului
- sprijin pentru îndeplinirea obligațiilor de raportare către finanțatorul proiectului, prin furnizarea informațiilor relevante cu privire la progresul proiectului, la solicitarea beneficiarului.

Metodologia de management de proiect propusă de furnizor va asigura:

- O structură bine definită de management al proiectului;
- Existenţa unor puncte flexibile de luare a deciziilor;
- Un sistem de planificare a resurselor şi a aspectelor de natură tehnică;
- Un set bine definit de proceduri de control;
- Managementul producerii livrabilelor proiectului.

Vor fi luate în considerare cel puţin următoarele procese de management de proiect:

- Asigurarea "direcţiei" proiectului;
- Planificare;
- Iniţializarea proiectului;
- Managementul limitelor etapelor;
- Controlul etapelor;
- Managementul activităţilor de producere a livrabilelor;
- Închiderea proiectului.

În termen de 30 de zile de la demararea proiectului, Prestatorul va prezenta raportul inițial însoțit de un set de documente de iniţializare a proiectului, cu următorul conţinut:

- Plan tehnic de implementare – descrierea tuturor activităţilor din graficul de execuţie Gantt, prezentarea obiectivelor etapelor, a informaţiilor necesare și a

celor rezultate, prezentarea structurii livrabilelor, prezentarea dependenţelor logice ale activităţilor și explicarea acestora;

- Plan de resurse – organigrama echipei Prestatorului, roluri și responsabilităţi, modalitatea de coordonare și raportare în cadrul echipei, interfeţe de comunicare cu beneficiarul;
- Plan de management al riscurilor – metodologia pentru managementul riscurilor (analiză, planificare, monitorizare), registrul riscurilor proiectului (identificare risc, cauze, efecte, modalitate de gestiune, plan de rezervă, responsabil);
- Plan de testare şi acceptanţă – strategia de testare (etape, obiective, formularistică, gestiunea procesului de testare);
- Plan de comunicare – strategia de raportare a proiectului, descriere rapoarte, frecvenţă, autor și destinatar;
- Plan de instruire – descrierea tuturor activităţilor de instruire planificate, număr sesiuni, tematică, participanţi, logistica furnizării instruirii, materiale furnizate, modalitatea de monitorizare a rezultatelor instruirii;
- Plan de asigurare a suportului în garanţie – modalitatea de asigurare a serviciilor de suport în perioada de garanţie, condiţii SLA.

O versiune iniţială a documentelor de iniţializare a proiectului va fi prezentată ca parte a ofertei tehnice.

5.2 Cerinţe specifice privind planificarea

Graficul de execuţie iniţial (cel ofertat) va fi salvat ca “baseline”, pentru a permite raportarea ulterioară a progresului comparativ cu versiunea iniţială. Graficul de execuţie va avea asociate coduri WBS (Work Breakdown Structure) pentru fiecare activitate, iar structura WBS va fi inclusă în baseline-ul salvat, astfel încât o activitate a proiectului să poată fi referită prin acelaşi cod WBS pe întreaga durată de execuţie a proiectului, indiferent de modificările pe care planul le poate suferi.

Următoarele informaţii vor fi obligatoriu incluse în graficul de execuţie:

- codul activităţii (WBS)
- Procentul de realizare (%)
- Denumirea activităţii (Task Name)
- Durata activităţii (Duration)
- Dependenţele activităţii (Predecessors)

- Entitatea responsabilă cu execuţia activităţii (Autoritatea Contractanta sau Ofertant)

Din punct de vedere grafic, planul va prezenta datele de start şi de finalizare pentru fiecare activitate. De asemenea, se va marca pe plan calea critică a proiectului.

Pentru raportarea periodică a progresului proiectului se va utiliza întotdeauna comparaţia cu planul salvat ca baseline.

Pe lângă activităţile pur tehnice, graficul de execuţie va include în toate situaţiile activităţile necesare pentru producerea livrabilelor scrise ale proiectului (rapoarte, manuale etc.), precum şi activităţile de avizare aferente acestora (împreună cu perioadele de timp necesare Autorității Contractante pentru avizarea lor). Termenul tipic necesar CERT-RO pentru avizarea unui livrabil scris va fi de aproximativ 5 zile lucrătoare (dacă nu este precizat altfel) şi va fi inclus ca atare în plan. Pentru a fi realiste, planurile vor include şi perioadele de timp necesare pentru încorporarea eventualelor comentarii ale Beneficiarului (sau pentru retestare, în cazul livrabilelor tehnice aferente soluției informatice).

Fiecare livrabil va fi marcat în mod distinct în plan, împreună cu activităţile aferente pentru producerea şi avizarea sa. Pentru orice livrabil se vor marca în plan cel puţin 2 milestone-uri: momentul predării livrabilului către CERT-RO pentru avizare /testare şi momentul avizării sale efective (acceptanţa). Prestatorul va pregăti planurile astfel încât să se asigure de faptul că termenele asumate prin contract pentru finalizarea unor activităţi includ şi timpii necesari pentru avizarea acestora şi pentru remedierea eventualelor neconformităţi. Un livrabil nu se va considera acceptat în momentul predării sale către Beneficiar în vederea avizării, ci numai după încorporarea eventualelor comentarii ale Beneficiarului (sau după finalizarea cu succes a testelor de acceptanţă stabilite în avans). Astfel, pentru livrabilele scrise pregătite de către Prestator se vor prevedea următoarele activităţi asociate procesului de acceptanţă:

- predarea livrabilului de către Prestator în vederea acceptanţei – milestone
- verificarea livrabilului de către Beneficiar și transmiterea unui punct de vedere – 5 zile lucrătoare
- încorporarea de către furnizor a feedback-ului într-o nouă versiune a livrabilului – 2 zile lucrătoare
- verificarea livrabilului de către Beneficiar și acordarea acceptanţei – 1-2 zile lucrătoare.

5.3 Cerinţe specifice privind monitorizarea progresului

5.3.1 Şedinţe de management

La nivelul echipei de proiect comune (CERT-RO – Prestator), se vor organiza şedinţe de monitorizare a stadiului proiectului cu o frecvenţă bi-lunară. Participanţii la aceste şedinţe vor fi:

- Liderul de echipă și, după caz managerul de proiect (pentru aspecte administrative și logistice) din partea Prestatorului;
- Managerul de proiect din echipa externă de implementare din partea CERT-RO
- Manager de proiect din echipa internă CERT-RO
- alți experți coordonatori implicați, din partea Prestatorului sau ai CERT-RO, dacă este cazul.

Aceste şedinţe vor avea o durată de maxim 2 ore şi vor avea drept obiectiv parcurgerea activităţilor planificate conform planului de etapă şi identificarea progresului realizării acestor activităţi. Se vor analiza activităţile finalizate, problemele apărute şi se vor planifica detaliat activităţile pentru perioada următoare. Pentru fiecare problemă apărută se vor stabili acţiuni de remediere, responsabilităţi şi termene de finalizare.

În cazul identificării unor probleme tehnice punctuale, acestea vor fi programate spre rezolvare în cadrul unor şedinţe tehnice. Rolul şedinţelor de management nu este acela de a găsi soluţii tehnice, ci de a stabili strategia de abordare a unor probleme sau de a lua decizii cu privire la activităţile proiectului sau la alocarea şi programarea activităţilor şi a resurselor).

În cadrul şedinţelor de management se pot discuta şi aspecte care ţin de registrul de riscuri al proiectului (monitorizarea unor riscuri deja identificate sau analiza şi planificarea unor riscuri nou identificate).

Prestatorul va asigura serviciile de secretariat în cadrul acestor şedinţe şi va pregăti minutele de discuţie în termen de max. 48 de ore de la data şedinţei. Minuta şedinţei va fi transmisă către toţi participanţii la şedinţă.

Prestatorul va întreţine un Registru de Acţiuni al proiectului, în care se vor înregistra toate acţiunile stabilite, responsabilii şi termenele agreate, precum şi istoricul rezolvării acestor acţiuni. Registrul de acţiuni actualizat va fi transmis tuturor participanţilor în termen de max. 48 de ore de la data şedinţei.

Cu cel puţin 24 de ore înainte de data programată a următoarei şedinţe, Managerul de proiect / Liderul de echipă al Prestatorului va transmite Responsabilului de proiect al Autoritatii Contractante și Managerului de proiect din echipa externă de implementare a CERT-RO Registrul de acţiuni actualizat cu progresul înregistrat al acţiunilor care se aflau în aria sa de responsabilitate. De asemenea, va transmite cu aceeaşi ocazie graficul de execuţie actualizat cu progresul la zi, ca bază pentru derularea şedinţei de monitorizare. Nu se vor organiza şedinţe de monitorizare în cazul în care nu există în prealabil un plan actualizat ca bază pentru discuţie.

5.3.2 Şedinţe tehnice ale echipei de proiect

La nivelul membrilor echipelor tehnice de proiect ale Autoritatii Contractante şi a furnizorului, se vor organiza periodic şedinţe de monitorizare tehnică a progresului sau de rezolvare a unor probleme tehnice apărute pe durata implementării proiectului. Frecvenţa acestor şedinţe va fi stabilită în funcţie de etapa proiectului şi de problemele care necesită rezolvare.

Toate materialele tehnice necesare pentru informarea participanţilor la şedinţă vor fi distribuite electronic acestora cu cel puţin 24 de ore înainte de data programată a şedinţei, pentru a le permite studierea materialelor în vederea unor discuţii şi decizii fundamentate.

Concluziile oricărei şedinţe tehnice vor fi documentate de către Prestator şi vor fi transmise către toţi participanţii spre confirmare în termen de maxim 48 de ore de la data şedinţei.

5.4 Cerinţe privind raportarea

Prestatorul este responsabil de elaborarea şi transmiterea următoarelor rapoarte către Autoritatea Contractantă:

Raportul Iniţial, la 30 de zile de la demararea execuţiei contractului. Raportul va specifica exact rezultatele de atins în cadrul fiecărei activităţi şi sarcinile care vor fi îndeplinite pentru atingerea rezultatelor. Acest document trebuie să cuprindă informaţii detaliate despre: planificarea activităţilor, metodologia utilizată, indicatorii care se doresc a fi obţinuţi, eventuale situaţii care vor influenţa implementarea acestuia, precum şi soluţii pentru posibile dificultati ce pot aparea in implementare.

De asemenea, Raportul iniţial trebuie să cuprindă informaţii despre experţii non-cheie, care vor fi mobilizati pentru implementarea activităţilor prevazute, programarea acţiunilor, perioada de timp alocată executării fiecărei activităţi.

Raportul iniţial va constitui principalul instrument de lucru şi se va face referire la el pe toată perioada de executare a contractului.

Rapoartele intermediare de progres trebuie să fie redactate la fiecare trei luni în timpul perioadei de execuţie a contractului. Acestea trebuie să fie însoţite de un raport financiar la zi (care trebuie să cuprindă detalii privind perioadele de timp efectuate de experţi şi alte cheltuieli conexe).

Aceste rapoarte vor detalia:

- Progresul general al proiectului
- Acţiuni derulate şi finalizate (nume şi cod WBS din graficul de execuţie)
- Acţiuni demarate şi aflate în execuţie (nume şi cod WBS din graficul de execuţie)
- Planul de milestones actualizat (milestones atinse sau întârziate)
- Rezultate realizate, livrabile finalizate şi stadiul acceptanţelor
- Resurse utilizate
- Acţiuni care se vor derula în următoarea perioadă de raportare
- dificultăţile întâmpinate în cursul implementării şi soluţiile propuse pentru a depăşi respectivele dificultăţi, riscuri şi planuri de tratare a acestora
- Graficul de execuţie actualizat, cu marcarea procentajului de îndeplinire pentru fiecare activitate şi vizualizare tip (Baseline) cu marcarea căii critice (actuals vs. baseline aprobat)
- Recomandări sau solicitări aferente

Raportul final va fi transmis Beneficiarului în termen de maxim 10 de zile de la sfârşitul contractului. O varianta preliminară a acestuia trebuie să fie transmisă cu cel puţin o lună înainte de sfârşitul perioadei de execuţie a contractului pentru a fi analizată. Raportul trebuie sa descrie întreg procesul de implementare şi va înlesni evaluarea rezultatelor obţinute atât în termeni calitativi, cât şi cantitativi.

Raportul va cuprinde descrierea rezultatelor obtinute, evaluarea succesului şi a constrângerilor majore pentru fiecare activitate şi sarcină, recomandări pentru acţiuni viitoare cu scopul asigurării durabilităţii activităţilor, rezultatele preconizate după finalizarea contractului, precum şi măsurile ce trebuie întreprinse de către Beneficiar în acest sens.

Raportul final trebuie însoţit de raportul financiar (care trebuie să cuprindă detalii privind perioadele de timp efectuate de experţi şi cheltuielile efectuate) precum şi copii ale facturilor şi/ sau contracte încheiate în vederea verificării eligibilităţii cheltuielilor conexe efectuate.

Facturile emise de Prestator vor fi transmise spre plata, numai in baza aprobării rapoartelor intermediare de progres/final si in urma semnarii proceselor verbale intermediare/final de

receptie/acceptanta a serviciilor. De asemenea, trebuie aprobate de catre Beneficiar toate fişele de prezenţă ale experţilor, pentru confirmarea realitatii volumului de munca efectuat.

În procesul de verificare a cheltuielilor conexe, altele decât cu onorariile experţilor, Beneficiarul poate solicita şi Prestatorul are obligaţia de a pune la dispoziţie documente justificative suplimentare, cum ar fi: liste de prezenţă, bilete de transport, diagramă cazare, copii după contracte şi facturi, minute, procese-verbale etc.

Pe parcursul derularii contractului, la solicitarea Beneficiarului, Prestatorul are obligatia de a prezenta si alte **rapoarte ad-hoc** relevante pentru implementarea proiectului, cum ar fi note explicative sau de sprijin, rapoarte de finalizare a unor activitati specifice, descrieri suplimentare etc, in functie de necesitati.

Toate rapoartele si documentele elaborate de către Prestator vor fi redactate în limba română. Toate rapoartele vor cuprinde o secţiune narativă de introducere şi o secţiune financiară si vor fi insotite de livrabilele prevazute in contract.

5.5 Facilităţi oferite de Beneficiar

Beneficiarul va asigura următoarele facilităţi Prestatorului, în vederea implementării, cât mai eficiente a contractului:

- sprijin tehnic prin contribuţia experţilor proprii la realizarea obiectivelor propuse prin proiect;
- sprijin în asigurarea unei comunicări eficiente cu toate părțile implicate, în vederea implementării cu succes a activităţilor proiectului;
- sprijin în stabilirea contactelor cu institutiile relevante şi în organizarea întâlnirilor cu persoanele reprezentative din cadrul entităţilor implicate;
- acces la sursele de informare disponibile: indicarea surselor pentru analiza documentara aferenta elaborarii setului de indicatori, date statistice privind criminalitatea informatica la nivel national si international, documente oficiale ale autorităţilor publice relevante etc.

6 Logistică și planificare

6.1 Locaţia

Baza proiectului va fi în Bucureşti, la sediul CERT-RO şi Prestatorului. Instruirea membrilor echipei Cyber Crime se poate face atat in tara, cat si in strainatate cu suportarea de catre prestator a costurilor aferente.

6.2 Data demarării şi Perioada de execuţie

Contractul va demara efectiv dupa data semnării acestuia de către Autoritatea contractantă şi Prestator, iar execuţia sa va începe la data notificării din partea Autorităţii contractante, nu mai târziu de 5 zile după semnare si constituirea garantiei de buna executie. Durata contractului este de **11 luni**.

7 Alte cerinţe

7.1 Cheltuieli conexe

Aceste cheltuieli acoperă costurile legate de instruirea si ceritificarea membrilor echipei Cyber Crime si secretariatului permanent, respectiv organizarea si sau participarea la evenimente de genul conferinte, seminarii, ateliere de lucru, reuniuni de lucru, cursuri de instruire, activitati transnationale, conform estimării bugetare.
Plafonul fix alocat acestor cheltuieli din cadrul contractului este de **1.320.000 lei fără TVA**.
Suma fixă alocată cheltuielilor conexe este inclusă în valoarea totală estimată fără TVA a contractului. Ofertantul nu poate să introducă în propunerea financiară, pentru cheltuielile conexe, o valoare mai mică sau mai mare decât plafonul indicat. De asemenea nu este obligatoriu a se cheltui în implementarea contractului întreaga sumă alocată acestor tipuri de cheltuieli.
Atenţie! Oferta care nu va respecta plafonul fix stabilit, va fi respinsă din cadrul procedurii de atribuire.
Aceste cheltuieli altele decât cu onorariile experţilor sunt necesare pentru a acoperi costurile legate de organizarea si sau participarea la evenimente de genul conferinte, seminarii, ateliere de lucru, reuniuni de lucru, cursuri de instruire, activitati transnationale şi pot fi decontate din plafonul în sumă fixă alocat acestor cheltuieli, dar numai după ce acesta a obţinut acordul scris al Autorităţii Contractante.
Aceste cheltuieli vor fi justificate de Prestator si decontate de Autoritatea Contractanta, prin prezentarea copiilor după facturile şi/sau contractele încheiate si alte documente justificative cum ar fi, dar fără a se limita la: liste participanţi, diagramă hotel, ordine de deplasare pentru participanţi, documente transport.
Cheltuielile aferente organizării şi participării la evenimente se vor face cu respectarea legislaţiei româneşti aflate în vigoare și aplicabile prezentului proiect şi reglementările privind eligibilitatea cheltuielilor în cadru PODCA.

8 Cerinţe speciale

Toate materialele elaborate în cadrul proiectului trebuie să conţină sigla Guvernului României, sigla UE şi sigla instrumentelor structurale în România, precum şi textul ”Proiect cofinanţat din FSE prin PODCA 2007-2013”.

Pentru mai multe detalii se va utiliza manualul de identitate vizuală pentru instrumente structurale 2007-2013 în România disponibil la adresa: http://www.fonduriadministratie.ro/Implementare_proiecte/Masuri_de_vizibilitate_PODCA