Propunere tehnica

Servicii de evaluare si de analiza a asigurarii calitatii sistemelor (servicii de testare a securitatii sistemului informatic al BNM)

Banca Nationala a Moldovei

27 octombrie 2022

Cuprins

Banca Nationala a Moldovei
Bucuresti, Romania

27 octombrie 2022

Stimati Domni,

Ca urmare a anuntului privind achizitia de servicii de evaluare si de analiza a asigurarii calitatii sistemelor (servicii de testare a securitatii sistemului informatic al BNM), suntem incantati sa va prezentam aceasta propunere pentru serviciile solicitate in cadrul Bancii Nationale a Moldovei.

Pentru realizarea acestui proiect, am alcatuit o echipa cu experienta semnificativa in furnizarea acestor servicii cu specialisti care au efectuat, pana in prezent, peste 600 de proiecte de audit similare.

Speram ca aceasta propunere sa indeplineasca asteptarile Dumneavoastra. Va rugam sa nu ezitati sa ne contactati daca aveti intrebari legate de propunerea noastra sau pentru a obtine orice alte informatii de care aveti nevoie.

Cu stima,

Cosmin Macaneata

Managing Partner

OMEGA Trust

COSMIN-MATEI MACANEATA

Digitally signed by COSMIN-MATEI MACANEATA
DN: cn=COSMIN-MATEI MACANEATA, sn=MACANEATA, givenName=COSMIN-MATEI, serialNumber=201104209CMM11, email=cosmin.macaneata@omega-trust.ro, o=OMEGA TRUST SRL, l=BUCURESTI SECTORUL 2, st=BUCURESTI, c=RO, title=ADMINISTRATOR
Date: 2022.10.27 09:33:48 +03'00'

1 Introducere

Banca Nationala a Moldovei (in continuare numita "BNM" sau "Beneficiarul"), intentioneaza sa achizitioneze servicii de evaluare a vulnerabilitatilor informatice si teste de penetrare in cadrul sistemului informatic.

In acest sens, Organizatia a transmis un anunt de participare privind achizitionarea serviciilor mai sus mentionate.

1.1 Obiectivul Dvs.

Obiectivul acestui proiect il reprezinta evaluarea nivelului de securitate al Sistemului Informatic al Bancii Nationale a Moldovei prin teste specifice specifice de penetrare din exteriorul infrastructurii de retea.

1.2 Aria de aplicabilitate

In conformitate cu specificatiile din caietul de sarcini, aria de aplicabilitate a activitatii noastre va cuprinde urmatoarele tipuri de activitati:

- Penetration testing a infrastructurii expuse in internet, inclusiv aplicatiile;
- Penetration testing a infrastructurii expuse in reteaua interbancara, inclusiv aplicatiile;
- Penetration testing a infrastructurii interne, avand la dispozitie un cont activ la o statie de lucru;
- Penetration testing a doua aplicatii accesibile doar din reteaua interna a BNM;
- Evaluarea vulnerabilitatii (vulnerability assessment) infrastructurii de retea inclusiv infrastructura wireless si penetrarea ei;
- Penetration testing a Sistemul automatizat de plati interbancare (SAPI) avînd acces la nivelul unui participant si a unui operator SAPI.

2 Indeplinirea cerintelor de calificare

In tabelul de mai jos, am rezumat cerintele de calificare ale achizitiei si mijloacele de indeplinire a acestora:

Cerinta	Indeplinirea cerintei
Garantie pentru oferta	Va rugam sa regasiti in ***Anexa A – Garantia pentru oferta***
Formularul DUAE	Va rugam sa regasiti in ***Anexa A – Formularul DUAE***
Declaratie privind valabilitatea ofertei (Anexa 8)	Va rugam sa regasiti in ***Anexa A declaratia solicitata***
Dovada înregistrarii persoanei juridice, în conformitate cu prevederile legale din tara în care ofertantul este stabilit - Certificat de inregistrare a intreprinderii/Extras din Registrul de stat al persoanelor juridice	Va rugam sa regasiti documentul solicitat in ***Anexa A***
Certificat de atribuire a contului bancar	Va rugam sa regasiti documentul solicitat in ***Anexa A***
Calitatea serviciilor prestate	Va rugam sa regasiti in ***Anexa A – certificarile ISO 9001 si ISO 27001***
Declaratia privind calitatea de participant la procedura (Anexa 15)	Va rugam sa regasiti documentul solicitat in ***Anexa A***
Raport financiar	Va rugam sa regasiti documentele solicitate in ***Anexa A***
Certificat cu privire la situatia contribuabilului	Va rugam sa regasiti documentul solicitat in ***Anexa A***
Certificat care confirma neaplicarea sanctiunilor penale (cazier juridic) fata de ofertant, precum si caziere judiciare pentru fiecare expert-cheie	Va rugam sa regasiti documentele solicitate in ***Anexa A***
Specificatii tehnice (Anexa nr. 1 la caietul de sarcini)	Va rugam sa regasiti ***in Anexa B*** *documentul solicitat*
Demonstrarea experientei operatorului economic in domeniul de activitate aferent obiectului contractului ce urmeaza a fi atribuit	Va rugam sa regasiti in ***Anexa B – Anexa 12 completata cu informatiile solicitate, precum si documentele justificative***
Valoarea minima (suma) a unui contract individual indeplinit pe parcursul perioadei indicate (numarul de ani)	Va rugam sa regasiti in ***Anexa B – Anexa 12 cu informatiile solicitate***
Demonstrarea accesului la infrastructura/ mijloacele indicate de autoritatea contractanta, pe care aceasta le considera strict necesare pentru indeplinirea corespunzatoare a Contractului	Va rugam sa regasiti in ***Anexa C – documentele de calificare ale expertilor cheie***
Formularul completat din Anexa nr.14	Va rugam sa regasiti in ***Anexa C – formularul nr. 14***

Ofertantul va specifica versiunile si producatorii pachetelor software care se vor folosi pentru prestarea serviciilor, de asemenea se vor atasa documente de la producatori în copie (file de catalog, prospecte, etc.) care sa contina caracteristicile produselor folosite. Se admite ca aceste documente sa fie prezentate în limba engleza.	Va rugam sa regasiti in ***Anexa D***, documentele solicitate.
Specificatii de pret	Va rugam sa regasiti atasat ***– Anexa nr. 2 – Pretul ofertei***

3 Prezentarea companiei

3.1 Informatii generale

OMEGA Trust este o companie romaneasca infiintata in 2004, specializata in furnizarea serviciilor de audit si consultanta in domeniul securitatii informatiei.

Din 2014, OMEGA Trust este parte a Nexia International, o organizatie mondiala de audit si consultanta plasata in top 10 la nivel mondial.

OMEGA Trust a dezvoltat o buna reputatie pentru furnizarea de servicii de o calitate excelenta pentru clientii care activeaza in domenii precum: Servicii Financiare, Telecom, Dezvoltare Software, Petrol si Gaze, Institutii Publice, Piete de Capital, Retail etc.

Omega Trust ofera servicii de audit si consultanta in securitatea informatiei de peste 11 ani, atat pentru companii locale, cat si straine. Avem o experienta semnificativa in sectorul bancar, oferind servicii de audit IT si servicii de teste de penetrare, atat pentru institutii bancare locale, cat si straine.

Cifrele noastre

800+	**600+**	**14 tari**
Proiecte	**Clienti**	**Servicii la nivel international**

Compania noastra a furnizat servicii de audit si consultanta IT pentru entitati importante din Romania si de peste hotare, cum ar fi:

Membrii echipei noastre detin o experienta semnificativa in domeniul auditului si consultantei IT, fiind implicati in proiecte de o larga diversitate, experienta care, de asemenea, este confirmata prin calificarile relevante si certificarile obtinute, printre care se numara:

Compania noastra detine atestate si certificari relevante pentru furnizarea serviciilor de audit si consultanta, printre care se numara:

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Auditor atestat de Securitate Cibernetica

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO
AUTORITATEA COMPETENTĂ LA NIVEL NAȚIONAL PENTRU SECURITATEA REȚELELOR ȘI SISTEMELOR INFORMATICE

ATESTAT

AUDITOR DE SECURITATE CIBERNETICĂ

seria CLE nr. 7011 din 24.08.2021

Tip atestat: ☑ General / ☐ Special / ☐ Comun

În aplicarea dispozițiilor art. 20 lit. p) din *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, cu modificările și completările ulterioare,

În temeiul prevederilor art. 12 din *Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică*, aprobat prin Ordinul secretarului general al Guvernului nr. 559/2021,

În baza *Raportului final de evaluare* nr. 4708/A13/2021, întocmit de Direcția Reglementare, Evidență, Autorizare și Monitorizare, în calitate de Autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice,

OMEGA TRUST SRL

cu sediul în: București, sector 2, Municipiul București; CUI: 16430500; registrul comerțului: J40/7943/2004, este atestat ca:

AUDITOR DE SECURITATE CIBERNETICĂ

Înscris în Registrul național al auditorilor de securitate cibernetică / IDASC: QC-FAB5A4.
Perioada de valabilitate: 24 august 2021 - 23 august 2024.

Dan CÎMPEAN
Director general

Petre Cimpean (Signature)
2021.08.25 12:48:17 +02'00'
2021.005.20060

Constantin CĂLIN
Director

DIRECTOR DREAM
Constantin CĂLIN

ROC/1213ME2

Auditor atestat in cadrul **Autoritatii pentru Digitalizarea Romaniei**

Auditor atestat in cadrul **Autoritatii de Supraveghere Financiara din Romania**

Auditor atestat conform **Regulamentului eIDAS**

3.2 Produse si servicii

OMEGA Trust furnizeaza servicii variate de audit si consultanta IT in functie de necesitatile clientilor. Cele mai frecvente servicii pe care le oferim clientilor nostri includ urmatoarele:

- **Servicii de audit IT**
  - Teste de penetrare la nivelul sistemelor informatice si infrastructurilor IT
  - Audit IT pentru sisteme de tip Internet/ Electronic/ Mobile Banking in conformitate cu cerintele Ordinului nr. 553/2019 emis de catre Ministerul Comunicatiilor si Societatii Informationale (MCSI);
  - Audit IT si servicii de evaluare a conformitatii cadrului de gestionare a rezilientei cibernetice in conformitate cu cerintele Regulamentului BNR nr. 3/2018;
  - Audit pentru conformitatea sistemelor Sent, Regis si Safir cu cerintele tehnice emise de Transfond si BNR (Audit IT pentru conexiunea cu Sistemul Electronic de Plati (SEP);
  - Audit de securitate pentru conformitatea cu Legea NIS(362/2018);
  - Audit IT pentru asigurarea conformitatii cu Decizia ADR 564/11.11.2021 pentru aprobarea Normelor privind reglementarea, recunoasterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanta utilizand mijloace video;
  - Audit IT pentru certificarea furnizorilor de servicii de incredere in conformitate cu prevederile Regulamentului UE 910/2014 (eIDAS);
  - Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022);
  - Audit de conformitate cu standardele ISO 27001, ISO 9001;
  - Audit IT pentru sisteme de arhivare electronica si autorizare a centrelor de date in conformitate cu Legea 135/2007;
  - Audit IT pentru acreditarea furnizorilor de servicii de certificare conform Ordinului nr. 473/09.06.2009 emis de catre Ministerul Comunicatiilor si Societatii Informationale (MCSI);
  - Audit IT conform reglementarilor emise de Autoritatea de Supraveghere Financiara (ASF);
  - Audit IT conform reglementarilor emise de catre institutiile pietei de capital din Romania;
  - Audit IT si servicii de evaluare a conformitatii cu cerintele GDPR;
  - Orice alt tip de audit IT de conformitate pentru certificarea faptului ca sistemele informatice din cadrul organizatiilor sunt conforme cu legislatia in vigoare si cu regulamentele aplicabile;
  - Audit al procedurilor si controalelor generale IT;

- Audit intern IT in functie de necesitatile entitatilor auditate.

- **Servicii de consultanta IT**
  - Asistenta in implementarea normelor de securitate cibernetica specificate de Legea NIS.
  - Servicii de consultanta IT pentru implementarea standardelor internationale precum ISO 27001 si a celor mai bune standarde de securitate din industrie;
  - Consultanta pentru dezvoltarea politicilor si procedurilor IT;
  - Consultanta pentru alinierea la prevederile GDPR;
  - Asistenta in implementarea aplicatiilor;
  - Dezvoltarea, implementarea si testarea Planurilor de Continuitate Operationala (BCP) si de Recuperare in Caz de Dezastru (DRP);
  - Analiza si imbunatatirea proceselor de business;
  - Managementul proiectelor IT;
  - Data mining.

4 Sumar executiv

BNM intentioneaza sa achizitioneze servicii de evaluare a vulnerabilitatilor informatice si teste de penetrare in cadrul sistemului informatic.

In acest sens, Organizatia a transmis un anunt de participare privind achizitionarea serviciilor mai sus mentionate.

Aceasta propunere tehnica face referire la evaluarea vulnerabilitatilor informatice ale sistemului informatic al BNM si teste de penetrare specific din interiorul infrastructurii de retea.

Obiectivul acestui proiect il reprezinta evaluarea nivelului de securitate al Sistemului Informatic al Bancii Nationale a Moldovei prin teste specifice specifice de penetrare din exteriorul infrastructurii de retea.

Proiectul se va desfasura respectand cerintele din caietul de sarcini si va fi realizat in trei etape: pre-evaluare, evaluare si post-evaluare, dupa cum urmeaza:

- **Etapa de Pre-evaluare (Pre-assesment)** - Aceasta reprezinta faza premergatoare a evaluarii vulnerabilitatilor si este necesara pentru determinarea specificatiilor precise si regulilor de desfasurare a evaluarii. In cadrul acestei etape vom stabili si elabora Planul de testare, Planul de actiuni (SOW – State of Work) precum si scenariile de atac si se vor obtine autorizatiile necesare desfasurarii testelor de penetrare.

- **Etapa de Evaluare (Assesment)** - Reprezinta etapa de identificare si evaluare a vulnerabilitatilor de securitate a sistemelor informatice. Aceasta etapa a testarii va include evaluarea conectivitatii intre sistemele utilizate pentru test si sistemele testate, culegerea informatiilor despre sistemele testate din domeniul public si privat, descoperirea sistemelor si serviciilor active precum si scanarea sistemelor pentru descoperirea vulnerabilitatilor.

- **Etapa de Post-evaluare (Post-assesment)** – In cadrul acestei etape, vom acorda suport Beneficiarului pentru intelegerea deplina a problemelor identificate si alegerea masurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), in scopul minimizarii riscurilor de securitate informatica asociate problemelor si vulnerabilitatilor descoperite si vom efectua un test de penetrare repetat la resursele cu probleme identificate pentru a verifica daca au fost aplicate corect masurile/metodele de remediere.

La finalul activitatilor, vom furniza livrabilele solicitate in caietul de sarcini. Continutul detaliat al livrabilelor noastre se regasesc in Sectiunea 5.3 – Livrabile.

In vederea unei bune desfasurari a proiectului este esentiala alocarea unor resurse disponibile din partea Beneficiarului care sa faciliteze accesul la resursele informationale necesare pentru realizarea testelor. In vederea preintampinarii unor eventuale probleme

in desfasurarea testelor, vom mentine o relatie permanenta cu reprezentantii Beneficiarului, pentru a semnala si rezolva in timp util eventualele dificultatile aparute.

Detaliile privind modalitatea de desfasurare a serviciilor se regasesc in capitolele urmatoare din propunerea tehnica.

5 Abordare si metodologie

Evaluarea vulnerabilitatilor informatice ale Sistemului Informatic se va realiza prin teste specifice de penetrare din interiorul infrastructurii de retea, care vor include:

- Penetration testing a infrastructurii expuse in internet, inclusiv aplicatiile;
- Penetration testing a infrastructurii expuse in reteaua interbancara, inclusiv aplicatiile;
- Penetration testing a infrastructurii interne, avand la dispozitie un cont activ la o statie de lucru;
- Penetration testing a doua aplicatii accesibile doar din reteaua interna a BNM;
- Evaluarea vulnerabilitatii (vulnerability assessment) infrastructurii de retea inclusiv infrastructura wireless si penetrarea ei;
- Penetration testing a Sistemul automatizat de plati interbancare (SAPI) avand acces la nivelul unui participant si a unui operator SAPI.

Prin intermediul testelor de penetrare vom evalua securitatea sistemului informatic prin simularea unui atac, prin exploatarea vulnerabilitatilor existente si cunoscute intr-un mod asemanator incercarilor de exploatare realizate de catre un atacator, cu diferenta ca acestea vor fi efectuate intr-un mod etic, cu permisiunea Beneficiarului. Procesul implica o analiza activa a sistemelor informatice pentru orice vulnerabilitati existente care ar putea rezulta din configuratia inadecvata si din brese cunoscute sau necunoscute, hardware si software.

Prin testarea securitatii sistemelor informatice se va asigura identificarea posibilelor vulnerabilitati existente la nivelul sistemelor hardware, bazelor de date si aplicatiilor software incorporate, furnizand echipelor, care asigura operarea, intretinerea si dezvoltarea acestora, informatii si recomandari destinate remedierii vulnerabilitatilor identificate.

Testele de penetrare vor analiza comportamentul sistemelor informatice in contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitatile care pot exista in aplicatiile dezvoltate sau utilizate. Un test de penetrare complet va cuprinde atat teste automate cat si manual, astfel:

- Testele automate vor identifica erori de programare in aplicatiile utilizate si vor fi efectuate cu ajutorul unor programe specializate precum instrumentele de scanare a vulnerabilitatilor, a aplicatiilor web si a codului, instrumente de testare si identificare a eventualelor erori de programare din aplicatii in vederea exploatarii lor;

- Testele manuale vor analiza aspecte ale aplicatiilor care necesita intuitia umana, identificandu-se erori logice de programare, si vor analiza si confirma sau infirma rezultatele testelor automate. Pentru atingerea acestor obiective, serviciile de penetrare si evaluare a vulnerabilitatilor informatice in cadrul Sistemului Informatic al BNM prin teste specifice de penetrare din exteriorul infrastructurii de retea.

Testele de penetrare vor avea ca rezultat o analiza complexa a securitatii sistemelor informatice ale BNM, testand eficacitatea masurilor de securitate implementate prin simularea atacurilor informatice. Activitatile noastre se vor baza pe practici de tip "ethical hacking", fiind luate in considerare urmatoarele scenarii:

A. **Black box** – in aceasta situatie echipa de testare nu va cunoaste nici o informatie despre sistemele auditate, cu exceptia informatiei de accesare a aplicatiilor (pagini web, adrese IP). Vom utiliza aceasta metoda pentru testarea infrastructurii externe a Beneficiarului;

B. **Grey box** – echipa de testare nu va cunoaste informatii despre sistemele auditate, va dispune de un cont de utilizator la o statie de lucru cu anumite roluri. Vom utiliza aceasta metoda pentru testarea infrastructurii interbancare si serviciilor disponibile, precum si a infrastructurii interne a BNM cu servicii aferente, definite in etapa de pre-evaluare (Pre-assessment). De asemenea, vom efectua testarea a doua aplicatii disponibile doar din reteaua interna a BNM si a (SAPI) avînd acces la nivelul unui participant SAPI si a unui operator SAPI.

Confirmam faptul ca vom utiliza echipamente si aplicatii si ca detinem experienta pentru realizarea testelor de penetrare la nivel de retea, inclusive wireless, sisteme de operare, baze de date si aplicatii, inclusive cele web, atacuri informatice simuland aplicatii malitioase, cat si de negare a serviciului (DoS, DDoS).

Confirmam faptul ca detinem si vom utiliza echipamente si aplicatii dedicate pentru identificarea si obtinerea informatiilor despre sistemele informatice tinta, identificarea de vulnerabilitati si formularea unor recomandari de remediere.

De asemenea, confirmam faptul ca detinem proceduri de lucru conforme standardelor in domeniu, prin care este redus riscul de a afecta sistemele informatice aflate in scopul testarii.

5.1 Activitatile desfasurate

Evaluarea vulnerabilitatilor si testele de penetrare se vor desfasura prin intermediul a trei etape distincte, si anume:

1. **Etapa de Pre-evaluare (Pre-assessment)**

   Aceasta reprezinta faza premergatoare a evaluarii vulnerabilitatilor si este necesara pentru determinarea specificatiilor precise si regulilor de desfasurare a evaluarii.

   In cadrul acestei etape, vom stabili si elabora Planul de testare, Planul de actiuni (SOW – State of Work) precum si scenariile de atac si se vor obtine autorizatiile necesare desfasurarii testelor de penetrare.

   Confirmam faptul ca aceasta etapa se va desfasura pe parcursul numarului de zile lucratoare stabilit in cadrul planului de proiect si se va finaliza cu elaborarea Planului de testare si a Planului de actiuni (SOW – State of Work) in care se vor inscrie cel putin:

   - activitatile intreprinse,
   - sistemele incluse in activitatea de testare,
   - termenul propus de realizare,
   - persoanele responsabile atat din partea Beneficiarului, cat si din partea noastra.

2. **Etapa de Evaluare (Assessment)**

   Reprezinta etapa de identificare si evaluare a vulnerabilitatilor de securitate a sistemelor informatice.

   Aceasta etapa a testarii va include evaluarea conectivitatii intre sistemele utilizate pentru test si sistemele testate, culegerea informatiilor despre sistemele testate din domeniul public si privat, descoperirea sistemelor si serviciilor active precum si scanarea sistemelor pentru descoperirea vulnerabilitatilor.

   Utilizand informatiile descoperite in evaluarea vulnerabilitatilor, se vor construi arbori de atac (attack trees) si se vor implementa actiunile definite in aceste structuri.

   Scanarea vulnerabilitatilor si implementarea testului de penetrare va include, dar nu se va limita la analiza urmatoarelor vulnerabilitati ale aplicatiilor web:

   - Injectarea de cod malitios;

- Managementul defectuos al procesului de autentificare si al sesiunii de lucru;
- Verificarea input-ului utilizatorului;
- Cross Site Scripting (XSS) ;
- Referentierea directa a obiectelor in mod nesecurizat;
- Erori privind configuratia de Securitate;
- Tratarea erorilor in mod nesecurizat si lipsa de masuri de protectie a informatiilor sensibile;
- Controale ineficiente privind managementul accesului;
- Cross-Site Request Forgery (CSRF);
- Utilizarea de componente de sistem cu vulnerabilitati cunoscute;
- Validarea parametrilor de intrare ai aplicatiilor;
- Comportamentul aplicatiilor/sistemelor aflate in scop la un atac de tip Denial of Service (DoS, DDoS)

Cu privire la managementul sesiunii de lucru, vor fi identificate cel putin urmatoarele aspecte:

- Implementarea managementului sesiunii printr-un framework cunoscut si de incredere, care a fost testat in practica din punct de vedere al securitatii.
- Procesul de generare a identificatorilor de sesiune si protectia acestora impotriva abuzurilor.
- Procesul de generare a cookie-urilor ce contin generatori de sesiune si stabilire a atributelor acestora.
- Procesul de creare si terminare a sesiunii si identificatorilor din perspectiva server si client.
- Intervaluri de inactivitate si posibilitatea de initializare de multiple sesiuni active.
- Masurile implementate pentru pastrarea confidentialitatii informatiilor privind autentificarea si sesiunea de lucru.
- Implementarea de masuri aditionale de securitate pentru operatiile sensibile, precum cele administrative

In privinta configuratiei de securitate, vom identifica cel putin urmatoarele aspecte:

- Versiunile de software ale serverelor, platformelor de dezvoltare a aplicatiei si componentelor sistemului
- Existenta actualizarilor de securitate aflate pe serverele, platformele de dezvoltare a aplicatiei si componentele sistemului.

- Existenta configuratiilor prestabilite de la producatorul sistemului, cum ar fi utilizatori si parole implicite.
- Utilizatorii de aplicatii si configuratia acestora.
- Metodele si extensiile protocolului HTTP folosite in cadrul sistemului.
- Informatii relevante ce se afla in header-ul HTTP.
- Existenta mecanismelor de criptare pentru autentificarea in cadrul sistemelor si transmisia de informatii

In privinta tratarii erorilor de sistem si protejarii informatiilor sensibile, vom identifica cel putin urmatoarele aspecte:

- Identificarea posibilitatii ca aplicatiile sa divulge informatii sensibile, inclusiv detalii despre sistem, identificatori de sesiune sau informatii despre cont, in mesaje de erori.
- Continutul mesajelor de eroare din punct de vedere tehnic

In privinta managementului accesului, vom identifica cel putin urmatoarele aspecte:

- Procesul de identificare, autentificare si autorizare a accesului la informatii.
- Identificarea credentialelor hard-codate in sisteme, daca acestea exista.
- Identificarea utilizatorilor si credentialelor de acces stocate in fisiere de configuratie in clar.
- Identificarea credentialelor transmise in clar, daca este cazul.
- Identificarea rolurilor de acces si maparea acestora pe drepturi si posibilitatea de ocolire a acestora pentru a obtine acces neautorizat la informatii.
- Identificarea metodelor HTTP folosite in procesul de autentificare.

In privinta validarii parametrilor de intrare, vom identifica cel putin urmatoarele aspecte:

- Filtrarea si validarea datelor provenite din afara sistemelor
- Existenta unei metode centralizate de validare a datelor in sistem.
- Existenta unor seturi de caractere corespunzatoare pentru datele de intrare
- Codificarea datelor intr-un set comun de caractere inainte de validare
- Validarea datelor provenite de la utilizatori, inainte de procesarea acestora, inclusiv toti parametrii, continutul URL si HTTP

Pentru validarea datelor de intrare se vor verifica:

- tipurile de date asteptate (integer, string etc,)

- setul de date
- lungimea datelor
- Implementarea de masuri suplimentare de control pentru caractere cu potential riscant (< > " ' % ( ) & + \ \' \")

Testarea securitatii la nivelul infrastructurii Wi-Fi va include, dar nu se va limita la:

- Descoperirea retelelor Wi-Fi si punctelor de acces atat cunoscute cat si neautorizate
- Identificarea dispozitivelor care interactioneaza cu reteaua
- Colectarea de informatii despre puterea de retea, protocoale de securitate si a dispozitivelor conectate
- Atacul si penetrarea retelelor criptate cu WEP, WPA-PSK si WPA2-PSK
- Impersonare SSID
- Atacuri de tip Man-in-the-middle (MITM)
- Monitorizare automata trafic pentru a gasi fluxuri de date sensibile
- Aderarea la retelele compromise si testarea sistemelor de backend
- Raportare cuprinzatoare a activitatilor de testare a retelelor de tip Wi-Fi

Scanarea vulnerabilitatilor si implementarea testului de penetrare la nivelul retelei va include, dar nu se va limita la:

- Obtinerea informatiilor din domeniul public;
- Scanarea sistemelor din SOW;
- Tehnici de enumerare;
- Obtinerea accesului neautorizat prin exploatarea vulnerabilitatilor;
- Consolidarea accesului;
- Stergerea tuturor fisierelor utilizate in cadrul atacului si a altor dovezi ale accesului.
- Aplicatii software utilizate in cursul testarii:
- Aplicatii pentru culegerea de informatii din domeniul public;
- Aplicatii necesare identificarii sistemelor si serviciilor active;
- Scannere de vulnerabilitati specifice sistemelor si retelelor incluse in Planul de actiuni (SOW - State of Work);
- Aplicatii necesare exploatarii vulnerabilitatilor descoperite

Prin testarea automata se vor detecta cel putin urmatoarele tipuri de vulnerabilitati:

- Parole initiale neschimbate pe echipamente
- Posibilitatea de acces in sistem fara autentificare, cu autentificare cu credentiale initiale sau credentiale usor de ghicit
- Configuratii initiale neschimbate pe echipamente
- Corectii si actualizari de securitate neimplementate
- Escaladarea privilegiilor
- Software cu versiuni vechi si foarte vechi ce prezinta vulnerabilitati
- Buffer Overflow
- Negarea accesului la serviciu (DoS Denial of Service)
- Remote Code Execution
- Posibilitatea injectarii de comenzi sau scripturi in servere web, servere de aplicatii si baze de date
- Directory Traversal
- File and Path Disclosure
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Configurarea defectuoasa a serverelor
- Managementul defectuos al sesiunilor si autentificarii
- Parametri de intrare nevalidati
- Control al accesului defectuos
- Tratarea defectuoasa a erorilor

Solutia de testare automata utilizata va fi capabila sa integreze capabilitatile de descoperire si remediere a vulnerabilitatilor cu informatii despre aplicatiile malware prezente in infrastructura, cat si toate aplicatiile malware cunoscute cu ajutorul carora se pot exploata vulnerabilitatile prezente si usurinta cu care aceste vulnerabilitati se pot exploata.

Aceasta etapa se va desfasura pe parcursul numarului de zile lucratoare stabilit in cadrul planului de proiect si se va finaliza cu elaborarea rapoartelor de test care vor include toate problemele si vulnerabilitatile descoperite pe parcursul testarii.

Va rugam sa regasiti in continuare o descriere a metodologiei utilizate pentru realizarea serviciilor. Activitatile se vor desfasura in cadrul a doua faze, dupa cum urmeaza:

- **Faza 1 – Evaluarea vulnerabilitatilor de securitate**

  In cadrul acestei faze, vom realiza o scanare a vulnerabilitatilor de securitate la nivelul sistemelor in scop.

  Acest proces se realizeaza prin utilizarea atat a uneltelor automate de scanare cat si a metodelor manuale de exploatare a sistemelor. Acest proces reprezinta un audit tehnic complet al sistemului prin identificarea punctuala a vulnerabilitatilor existente precum si a metodelor de corectare a acestora.

  Daca va fi aplicabil, cel putin urmatoarele vulnerabilitati vor fi evaluate:

  - Cele mai frecvente 10 riscuri de securitate pentru aplicatiile web conform ierarhizarii OWASP (pentru a nu denatura sensul, am pastrat denumirile in limba engleza):
    - A01 Broken Access Control
    - A02 Cryptographic Failures
    - A03 Injection
    - A04 Insecure Design
    - A05 Security Misconfiguration
    - A06 Vulnerable and Outdated Components
    - A07 Identification and Authentication Failures
    - A08 Software and Data Integrity Failures
    - A09 Security Logging and Monitoring Failures
    - A10 Server-Side Request Forgery
  - Cele mai frecvente 25 de riscuri de securitate pentru aplicatiile web conform ierarhizarii CWE Top 25 Most Dangerous Software Weaknesses (pentru a nu denatura sensul, am pastrat denumirile in limba engleza)
    - CWE-787 Out-of-bounds Write
    - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
    - CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
    - CWE-20 Improper Input Validation
    - CWE-125 Out-of-bounds Read
    - CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
    - CWE-416 Use After Free

-	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
-	CWE-352	Cross-Site Request Forgery (CSRF)
-	CWE-434	Unrestricted Upload of File with Dangerous Type
-	CWE-476	NULL Pointer Dereference
-	CWE-502	Deserialization of Untrusted Data
-	CWE-190	Integer Overflow or Wraparound
-	CWE-287	Improper Authentication
-	CWE-798	Use of Hard-coded Credentials
-	CWE-862	Missing Authorization
-	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
-	CWE-306	Missing Authentication for Critical Function
-	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
-	CWE-276	Incorrect Default Permissions
-	CWE-918	Server-Side Request Forgery (SSRF)
-	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
-	CWE-400	Uncontrolled Resource Consumption
-	CWE-611	Improper Restriction of XML External Entity Reference
-	CWE-94	Improper Control of Generation of Code ('Code Injection')

Evaluarea vulnerabilitatilor se va realiza in urmatorii pasi:

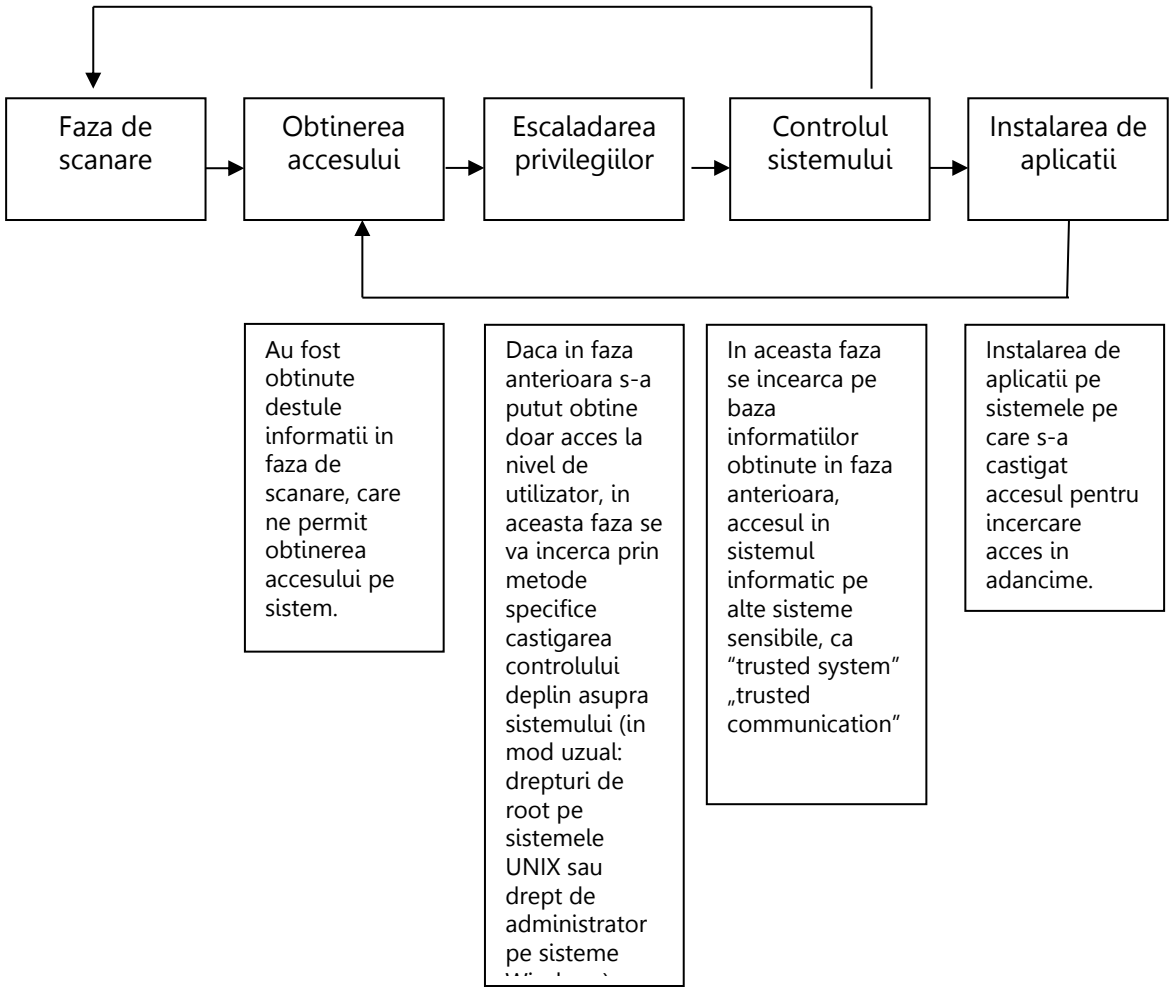
Analiza topologiei retelei	Se alcatuieste harta retelei (adrese IP, routere, switch-uri, server VLAN-uri, conexiuni Internet si VPN etc.)
Identificarea echipamentelor de retea si a configuratiilor	Aceasta activitate implica identificarea device-urilor de tip Firewall/ Router si a regulile de acces ACL.
Profilare sisteme/ echipamente	Identificarea sistemelor de operare in scopul efectuarii testelor adresate vulnerabilitatilor asociate fiecarui sistem de operare in parte. Identificarea sistemelor de operare se face prin scanarea de tip OS Fingerprint si citirea banner-elor anumitor servicii specifice fiecarui sistem de operare.
Profilare servicii	Identificarea serviciilor active si a versiunilor acestora in scopul efectuarii testelor adresate vulnerabilitatilor asociate fiecarui serviciu in parte. Identificarea serviciilor active se va face prin citirea banner-elor acestora sau prin analiza pachetelor TCP sau UDP returnate de respectivele servicii.
Scanare vulnerabilitati - automata	Dupa ce s-a realizat inventarierea sistemelor de operare si a serviciilor active pe fiecare sistem in parte, se va realiza identificarea automata a vulnerabilitatilor de pe sistemele respective. Acest lucru se va realiza prin utilizarea unor unelte specializate.

- **Faza 2 – Teste de penetrare**

  Dupa ce potentialele vulnerabilitati au fost descoperite ca parte a etapei anterioare, vom realiza teste de penetrare prin care vom incerca sa jucam rolul unui atacator care incearca sa obtina acces neautorizat la sistemele informatice si la datele administrate cu ajutorul acestora. Aceste teste vor avea rolul de a confirma daca vulnerabilitatile identificate pot fi intr-adevar exploatate de un hacker.

  In cadrul testelor noastre, vom utiliza ca referinta standardul nominal pentru vulnerabilitati informatice (CVE), precum si criteriile definite prin cadrele de testare a securitatii sistemelor informatice OSSTM (Open Source Security Testing Methodology Manual) si ISSAF (Information Systems Security Assessment Framework).

  Prezentam in continuare schema realizarii unui test de penetrare:



Testele de penetrare vor fi realizate in urmatorii pasi:

Testare de securitate	Dupa ce potentialele vulnerabilitati au fost descoperite, utilizand unelte specializate de scanare a sistemelor, interventia manuala este necesara pentru a confirma existenta efectiva a respectivelor vulnerabilitati. Astfel este redus nivelul alertelor de tip "false positive". Validarea vulnerabilitatilor consta in efectuarea de teste de exploatare a acestora folosind unelte specifice (exploit). Exploatarea serviciilor vulnerabile se face prin metode de tip buffer-overflow (necesita rularea de exploit-uri). Pe sistemele pe care a fost posibil accesul cu drepturi de utilizator, se va incerca exploatarea locala pentru a prelua controlul total (sau aproape total) asupra sistemului. Sistemele compromise pot fi folosite ca surse ale atacurilor ulterioare.
Testare metode autentificare	Vor fi testate mecanismele de autentificare ale utilizatorilor sau ale aplicatiilor in scopul evidentierii riscurilor de preluare a accesului sau nerespectare a politicii de securitate a accesului. In cadrul acestor teste este necesara monitorizarea si interceptarea comunicatiilor de retea si preluarea de parole "in clar" transmise prin medii necriptate.
Testare configuratie	Vor fi testate posibile erori de configurare ale aplicatiei precum si verificarea setarilor implicite
Testare politica securitate/ drepturi acces	Testarea drepturilor in aplicatie din perspectiva mai multor niveluri de acces (vizitator, utilizator, administrator etc.)
Testare detaliata a aplicatiei impotriva atacurilor specifice	Testarea detaliata a aplicatiilor impotriva vulnerabilitatilor identificate ca parte a sub-modulului anterior (SQL injection, cross-site scripting (XSS), brute-force, buffer overflow etc.)

Aceste teste vor fi realizate cu ajutorul instrumentelor specializate sau prin investigare manuala.

Vulnerabilitatile identificate vor fi descrise detaliat in raportul de securitate impreuna cu recomandarile noastre de remediere.

Toate vulnerabilitatile si riscurile identificate vor fi clasificate in functie de probabilitate, impact si risc, utilizand metodologia de mai jos:

VALOARE SEVERITATE (IMPACT TEHNIC) Impactul negativ asupra informatiei gestionate de aplicatie si sistem, pierdere sau degradare sau o combinatie a acestora a urmatoarelor obiective ale securitatii: integritate, disponibilitate, confidentialitate.	**NIVEL**	**SCOR**	**DESCRIERE**
	SCAZUT	1-5	Afectarea limitata a informatiilor sau sistemului; obtinerea de informatii utile pentru generarea unor atacuri.
	MEDIU	6-14	Afectarea semnificativa a informatiilor sau sistemului; pierdere de informatii; indisponibilitate serviciu; acces limitat la sistem.
	SEVER	15-20	Pierderi foarte importante ale informatiei, acces nelimitat la sistem; prejudicii la nivelul organizatiei.
VALOARE PROBABILITATE Probabilitatea ca o anumita vulnerabilitate sa fie exploatata de catre un atacator. La calcularea probabilitatii se au in vedere: motivatia atacatorului, nivelul de cunostinte necesar, usurinta in detectare si exploatare a vulnerabilitatii, nivelul de acces necesar si existenta unor masuri de detectie si prevenire.	**NIVEL**	**SCOR**	**DESCRIERE**
	FOARTE MICA	1	Vulnerabilitatea nu este direct exploatabila
	MICA	2	Vulnerabilitatea necesita un efort semnificativ si cunostinte avansate pentru a fi exploatata manual. Atacatorul ar putea avea nevoie de acces si cunostinte interne ale sistemului.
	MEDIE	3	Vulnerabilitatea necesita cunostinte specifice si poate fi exploatata cu instrumente disponibile public.
	MARE	4	Vulnerabilitatea necesita anumite cunostinte si poate fi exploatata fara instrumente speciale sau foarte usor de gasit si utilizat.
	FOARTE MARE	5	Vulnerabilitatea necesita anumite cunostinte si poate fi exploatata fara instrumente speciale sau foarte usor de gasit si utilizat.

NIVEL RISC = VALOARE SEVERITATE (IMPACT) x VALOARE PROBABILITATE

NIVEL RISC	VALOARE	MASURI NECESARE

MAXIM	**75 – 100**	Actiune imediata pentru reducerea nivelului de risc
CRITIC	**25 – 74**	Implementare de masuri corective cat mai curand posibil
MEDIU	**5 - 24**	Implementare de masuri corective intr-o perioada rezonabila de timp
SCAZUT	**2 - 4**	Pot fi implementate anumite masuri corective sau se accepta riscul
INFORMATIONAL	**1**	Reprezinta o observatie care nu determina un risc de securitate

3. Etapa de Post-evaluare (Post-assessment)

Aceasta etapa se va desfasura pe parcursul numarului de zile lucratoare stabilit in cadrul planului de proiect si se va finaliza cu elaborarea de catre Omega Trust a rapoartelor de analiza, a rezultatelor testelor efectuate in care se vor identifica si vor fi incluse cele mai bune masuri si metode de remediere a problemelor si vulnerabilitatilor descoperite, in functie de severitate si impact.

In cadrul acestei etape, vom acorda suport Beneficiarului pentru intelegerea deplina a problemelor identificate si alegerea masurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), in scopul minimizarii riscurilor de securitate informatica asociate problemelor si vulnerabilitatilor descoperite.

Totodata, vom efectua un test de penetrare repetat la resursele cu probleme identificate pentru a verifica daca au fost aplicate corect masurile/metodele de remediere.

5.2 Instrumente pentru efectuarea testelor

Evaluarea vulnerabilitatilor informatice se va realiza prin folosirea unor software specifice precum:

- Nexpose (https://www.rapid7.com/)
- Burp Suite Professional (https://portswigger.net/)
- Distributia Kali Linux Distribution (https://www.kali.org/docs/).

Trebuie mentionat ca distributia Kali Linux contine multiple instrumente open source care sunt folosite in evaluarea securitatii.

Documentatia de prezentare aferenta produselor folosite se regaseste la adresele web indicate mai sus si pentru solutia Nexpose si Burp Suite Professional au fost atasate fisele de produs la **Anexa D** a acestui document.

Compania noastra isi asuma raspunderea legalitatii utilizarii instrumentelor folosite in cadrul proiectului si, inainte de inceperea activitatii, va prezenta Beneficiarului dovada utilizarii legale a acestora.

5.3 Livrabile

In conformitate cu solicitarile Dvs, livrabilele noastre vor include in mod obligatoriu:

- Planul de proiect detaliat;
- Planul de testare;
- Planul de actiuni (SOW – State of Work);
- Rapoarte de test care vor include toate problemele si vulnerabilitatile detectate pe parcursul testarii, catalogate in functie de gravitatea lor;
- Rapoarte de analiza, continand analiza rezultatelor testelor efectuate in care se vor identifica si vor fi incluse recomandari de remediere continand cele mai bune actiuni/masuri/metode ce trebuie intreprinse/luate/folosite pentru eliminarea sau micsorarea riscului generat de vulnerabilitatile detectate.

Rapoartele furnizate vor fi structurate in doua parti distincte: partea executiva si partea tehnica.

Partea executiva va contine descrierea pe scurt a problemelor si vulnerabilitatilor identificate si va utiliza metode grafice (cel putin diagrame, grafice sau harti).

Partea tehnica va detalia din punct de vedere tehnic problemele si vulnerabilitatile identificate.

Partea tehnica va contine cel putin urmatoarele capitole:

- Sumar executiv;
- Obiectivele si scopul evaluarii;
- Prezentarea metodologiei utilizate in cadrul testarii;
- Descrierea contextului in care s-a desfasurat testarea;
- Detalii despre reteaua si sistemele evaluate:
    - echipamentele si serviciile active (adrese IP, porturi deschise)
    - Tipul, versiunea, statusul actualizarilor aplicatiilor

- Sistemul de operare

- Prezentarea individuala a vulnerabilitatilor descoperite, dupa cum urmeaza:
  - descrierea vulnerabilitatii;
  - catalogarea vulnerabilitatii;
  - descrierea tehnica;
  - analiza severitatii si probabilitatii;
  - calcularea riscului;
  - contramasuri recomandate pentru remediere.
- Alte detalii si recomandari;
- Anexa cu lista testelor de securitate efectuate.

Recomandarile de remediere a problemelor si vulnerabilitatilor identificate vor cuprinde cele mai bune actiuni/masuri/metode ce trebuie intreprinse/luate/folosite pentru eliminarea sau micsorarea riscului generat de problemele si vulnerabilitatile detectate precum si recomandari si propuneri de implementare ale acestora.

Livrabilele noastre vor fi discutate cu reprezentantii Beneficiarului si orice remarci agreate, adaugiri sau corecturi vor fi incorporate in varianta finala a acestora ce va fi emisa ulterior.

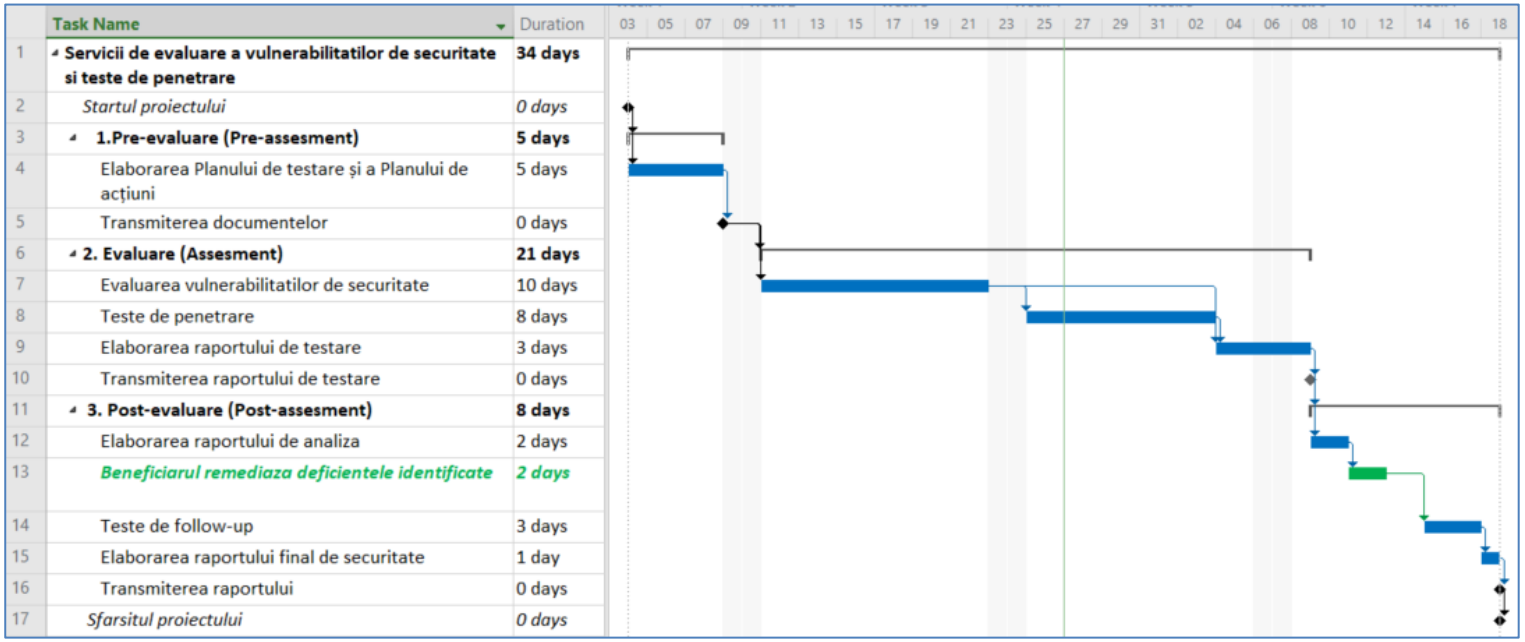
Livrabilele noastre vor fi furnizate in limba romana sau engleza.

Va rugam sa regasiti in **Anexa E**, un model al Raportului care va fi inaintat Beneficiarului.

6 Managementul proiectului

6.1 Planul de proiect

Puteti gasi mai jos o reprezentare grafica a planului de proiect. Data exacta de inceput va fi stabilita impreuna cu conducerea BNM.



	Task Name	Duration
1	**Servicii de evaluare a vulnerabilitatilor de securitate si teste de penetrare**	**34 days**
2	*Startul proiectului*	*0 days*
3	**1.Pre-evaluare (Pre-assesment)**	**5 days**
4	Elaborarea Planului de testare și a Planului de acțiuni	5 days
5	Transmiterea documentelor	0 days
6	**2. Evaluare (Assesment)**	**21 days**
7	Evaluarea vulnerabilitatilor de securitate	10 days
8	Teste de penetrare	8 days
9	Elaborarea raportului de testare	3 days
10	Transmiterea raportului de testare	0 days
11	**3. Post-evaluare (Post-assesment)**	**8 days**
12	Elaborarea raportului de analiza	2 days
13	***Beneficiarul remediaza deficientele identificate***	***2 days***
14	Teste de follow-up	3 days
15	Elaborarea raportului final de securitate	1 day
16	Transmiterea raportului	0 days
17	*Sfarsitul proiectului*	*0 days*

6.2 Gestionarea proiectului

Pentru o buna desfasurare a proiectului, vom indeplini toate cerintele cu respectarea si aplicarea celor mai bune practici in domeniu.

Pentru implementarea in timp si cu succes a proiectului, vom asigura furnizarea de informatii, date si obtinerea in timp util a oricaror comentarii/ constatari cu privire la documentele produse.

Proiectul va urma metodologia noastra interna de management, adaptata la specificul acestui proiect. Aceasta este o combinatie de management de proiect Agile si principiile PMBOK. Abordarea de management va urma pasii urmatori:

- **Initierea si planificarea proiectului**. Dupa atribuirea contractului, vom finaliza echipa de proiect si vom organiza o intalnire initiala impreuna cu Beneficiarul, in cadrul careia vom prezenta echipa si vom conveni asupra planului de activitati.

  In faza de planificare, vom defini un plan de comunicare, care va include intalniri programate, programul de livrare si formatul documentelor de raportare a progresului.

  Vom discuta si vom decide asupra sabloanelor de documente care vor fi utilizate pentru livrabilele si alte documente produse in timpul executiei proiectului.

- **Executia proiectului**. In faza de executie a proiectului, vom executa sarcinile si activitatile stabilite, in termenele convenite. Orice riscuri care nu au fost identificate la initierea proiectului vor fi comunicate Beneficiarului in timp util, pentru a identifica actiunile adecvate de control.

  Toate livrabilele vor fi verificate pentru acuratete si calitate. OMEGA Trust utilizeaza o metodologie interna de asigurare a calitatii, folosind cel putin doua niveluri de revizuire a muncii, precum si a rezultatelor preconizate, care urmeaza sa fie trimise la Beneficiar, pentru a se asigura ca documentatia si lucrarile efectuate sunt de cea mai inalta calitate. Astfel, fiecare raport sau livrabil este revizuit de o persoana cu abilitati de revizuire si de un nivel superior.

  In calitate de Manager de proiect a fost asignat insasi directorul general al Omega Trust care va fi implicat in revizuirea livrabilelor.

- **Monitorizarea si controlul proiectului.** Pe intregul parcurs, proiectul va fi monitorizat in raport cu planul stabilit. Dupa identificarea unei probleme, actiunile corective sunt planificate si gestionate pana la inchidere.

Vom desfasura periodic intalniri interne privind stadiul proiectului, in cadrul carora vom revizui progresul proiectului, etapele de referinta, orice riscuri sau probleme identificate si starea oricaror actiuni corective.

Vom asigura alocarea de resurse umane competente, familiarizate pe deplin cu sarcinile primite si ne vom asigura in permanenta de disponibilitatea resurselor corespunzatoare pentru realizarea activitatilor prevazute in caietul de sarcini.

Vom informa Beneficiarul permanent si in mod corect despre evolutia contractului.

Prin semnarea contractului de servicii, recunoastem atat importanta serviciilor pe care trebuie sa le furnizam, cat si constrangerile legate de termenele din graficul de implementare a activitatilor proiectului.

Vom adopta o atitudine constructiva (pro-activa) in indeplinirea obiectivelor contractului, aceasta insemnand cel putin urmatoarele:

- vom demonstra capacitatea de a ne adapta modificarilor din proiectul in care suntem implicati;

- vom elabora raportarile intr-un format agreat anterior cu Beneficiarul, in care informatiile furnizate vor fi complete, precise, clare, exacte si fara ambiguitati, cu atentie la detalii si accesibilitate.

Vom pune la dispozitia Beneficiarului toate documentele realizate in cadrul contractului, acestea intrand in proprietatea exclusiva a celui din urma.

Vom asigura pastrarea confidentialitatii documentelor, materialelor, datelor si informatiilor in legatura cu proiectul, care au fost indicate de catre Beneficiar ca fiind confidentiale.

6.3 Plan de gestionare a riscurilor

Va rugam sa regasiti mai jos modul nostru de abordare a activitatii de identificare a riscurilor, diminuare a acestora, precum si modul de prevenire/atenuare/eliminare sau minimizare a efectelor:

Nr.crt.	***Riscurile identificate de catre Ofertant***	***Masurile propuse de catre Ofertant ca parte a strategiei de risc*** (prevenirea/atenuare a/eliminarea riscurilor identificate)
1.	Dificultati de colaborare si comunicare intre factorii interesati implicati	- Stabilirea unor persoane dedicate, atat din partea Omega Trust cat si din partea Beneficiarului care sa tina legatura si sa faca toate comunicarile dintre parti. Aceste persoane vor trebui sa dovedeasca o buna cunoastere atat a procedurilor care urmeaza a le efectua echipa de experti asigurandu-se astfel posibilitatea respectarii termenelor ce vor trebui sa fie convenite. - Alocarea unui Project Manager de ambele parti.
2.	Datele si informatiile necesare desfasurarii serviciilor, comunicate de catre Beneficiar nu sunt suficiente pentru indeplinirea cerintelor solicitate prin Caietul de Sarcini la nivelul de calitate asteptat	- Stabilirea unor persoane dedicate, atat din partea Omega Trust cat si din partea Beneficiarului care sa tina legatura si sa faca toate comunicarile dintre parti. Aceste persoane vor avea responsabilitatea obtinerii informatiilor corecte, concrete si complete. - Solicitari de informatii clare si detaliate
3.	Aparitia necesitatii de adaugare a unor activitati/ solicitari de informatii noi, in functie de progresul activitatilor	Vom raspunde solicitarilor prin alocarea de resurse necesare (atat umane cat materiale)

4.	Personal insuficient sau diferente de intelegere a notiunilor din caietul de sarcini, pentru indeplinirea cerintelor solicitate la nivelul de calitate asteptat;	Fiecare expert al Omega Trust este instruit cu privire la obiectul contractului si ne asiguram, inca din procesul de selectie al expertilor, ca acestia indeplinesc toate cerintele din punct de vedere al calificarilor si al competentelor.
5.	Incarcatura mare de lucru a personalului din cadrul Beneficiarului ce ar putea crea dificultati in desfasurarea activitatilor din proiect	Planificarea programului de lucru astfel incat orarul activitatilor sa fie favorabil ambelor parti
6.	Intarzieri in finalizarea si predarea livrabilelor	- Desemnarea unui coordonator de proiect care sa supervizeze buna desfasurare a serviciilor si incadrarea in termenele prestabilite; - Organizarea riguroasa a activitatilor prin utilizarea de instrumente de management de proiect; - Realizarea corecta si la timp a raportarilor.

6.4 Plan de management al calitatii

OMEGA Trust utilizeaza o metodologie interna de asigurare a calitatii, folosind cel putin doua niveluri de revizuire a muncii, precum si a rezultatelor preconizate, care urmeaza sa fie trimise la clienti, pentru a se asigura ca documentatia si lucrarile efectuate sunt de cea mai inalta calitate. Astfel, fiecare raport sau livrabil este revizuit de o persoana cu abilitati de revizuire si de un nivel superior.

Pe toata durata derularii contractului, proiectul va fi monitorizat conform planului stabilit. In cazul identificarii unei deviatii de la planul de proiect, vom lua masurile corective adecvate, care vor fi planificate si gestionate pana la inchiderea lor.

De asemenea, compania noastra detine certificarea ISO 9001:2008 in managementul calitatii eliberat de catre United Registrar of Systems, organism acreditat international de catre UKAS. Ca rezultat al implementarii sistemului de management al calitatii, am obtinut o optimizare a proceselor operationale, o imbunatatire din punct de vedere calitativ a serviciilor oferite si, cel mai important, cresterea satisfactiei clientilor si colaboratorilor nostri.

In plus, Compania noastra detine si certificarea ISO 27001 in managementul securitatii informatiilor eliberata de United Registrar of Systems.

6.5 Echipa de proiect

Activitatile din cadrul proiectului se vor realiza cu resursele puse la dispozitie de catre Omega Trust, avand la baza informatiile specifice sistemelor din aria de aplicabilitate a testelor de penetrare.

Astfel, Omega Trust a nominalizat in cadrul echipei de proiect personal calificat si experimentat, in vederea atingerii obiectivelor si rezultatelor contractului

Va prezentam in continuare membrii cheie ai echipei care va fi implicata in activitatea acestui proiect.

Cosmin Macaneata – Expert cheie 1 - Manager de proiect

Cosmin Macaneata este Director General al companiei noastre si va actiona in cadrul proiectului in calitate de Manager de proiect.

Inainte de a lucra la Omega Trust, Cosmin a lucrat 5 ani intr-o companie multinationala de audit, unde a coordonat echipele Departamentului IT Advisory in numeroase proiecte de Audit si Consultanta IT.

Cosmin are o vasta experienta in domeniu, fiind responsabil cu efectuarea si coordonarea unui numar de peste 700 de proiecte de consultanta si audit IT.

Pana in prezent Cosmin a fost implicat in proiecte precum: evaluarea vulnerabilitatilor de securitate si teste de penetrare, audituri de securitate pentru infrastructura IT, audituri pentru sisteme de tip sisteme de tip internet/ home/ mobile banking, audituri de securitate pentru infrastructura SWIFT, audit de Securitate cnform Legii NIS, auditarea cerintelor impuse de Ordinul MCSI Nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plata electronica cu acces la distanta, audituri pentru verificarea indeplinirii conditiilor de autorizare a centrului de date, implementarea sistemelor de management al securitatii informatiilor conform standardului ISO 27001:2013, revizuiri de procese si controale IT in conformitate cu cele mai bune practici din industrie sau diverse standarde (cum ar fi ISO/IEC 27002, ISO 27001:2013, ITIL, COBIT, ISACA etc.), audituri pentru conformitatea cu cerintele GDPR, audituri interne IT, audituri de functionalitate pentru sisteme de tip Enterprise Resource Management (ERP) sau audituri de migrare a datelor utilizand Tehnici de Audit Asistate de Calculator (CAATs).

De asemenea, Cosmin a fost implicat in proiecte de consultanta, cum ar fi: elaborarea si revizuirea procedurilor operationale si de securitate IT pentru conformitatea cu standardul ISO 27001, consultanta in implementarea cerintelor tehnice si operationale ale GDPR, dezvoltarea specificatiilor functionale pentru implementarea unor sisteme informatice, analiza proceselor de business, implementarea unor sisteme pentru detectarea fraudelor, analize de date, elaborarea si implementarea planurilor de continuitate operationala si de recuperare in caz de dezastru, etc.

Experienta lui este legata de sisteme informatice foarte variate, incluzand sisteme de plati: sisteme de Internet Banking, Home Banking, Mobile Banking, SWIFT etc. Alte sisteme informatice de care este legata activitatea lui Cosmin sunt: sisteme de tip ERP (SAP, SIVECO Applications, BAAN, JD Edwards, Microsoft Navision, Charisma Enterprise sau Oracle E-business suite). Pana in prezent, Cosmin a furnizat servicii IT pentru mai mult de 500 de companii din mai multe industrii, cum ar fi: industria bancara, piete de capital, Telecomunicatii, Retail, Oil&Gas si Industria Producatoare.

Cosmin a absolvit facultatea de Cibernetica Statistica si Informatica Economica din cadrul ASE Bucuresti si a absolvit cursurile unui Masterat in Managementul sistemelor informatice, in cadrul Facultatii de Cibernetica Statistica si Informatica Economica.

De asemenea, Cosmin ocupa functia de Manager al Departamentului de Management al Securitatii Informatice in cadrul companiei Omega Trust din anul 2010.

Cosmin detine urmatoarele certificari:

- **Manager de proiect cod COR 242101;**
- **CISA (Certified Information Systems Auditor);**
- **CIPM (Certified Information Privacy Manager).**
- CEH v10 (Certified Ethical Hacker);
- Auditor de securitate cibernetica, atestat emis de catre DNSC;
- ISO 27001 Lead Auditor;
- ISO 27005 Risk Manager;
- DPO (Data Protection Officer).

Dan Sora – Expert cheie 2 - Expert sef securitate sisteme informatice

Dan Sora va actiona in cadrul echipei in calitate de Expert sef securitate. Dan lucreaza cu noi de 12 ani, timp in care a fost implicat in numeroase proiecte de audit si consultanta IT.

Dintre proiectele in care Dan a fost implicat amintim: audituri pentru certificarea furnizorilor de servicii de incredere in conformitate cu legislatia nationala si europeana, audituri pentru aplicatii de tip Internet, Mobile si Phone Banking respectand legislatia Ministerului Comunicatiilor si Societatii Informationale, teste de penetrare interne si externe, audituri de securitate pentru infrastructura IT, audituri de securitate pentru infrastructura SWIFT, audituri pentru Sistemul Electronic de Plati (SEP), audituri tehnice pentru sisteme informatice finantate din fonduri europene, revizuiri de procese si controale IT in conformitate cu cele mai bune practici din industrie sau audituri de functionalitate pentru sisteme de tip Enterprise Resource Management (ERP).

Ca parte a proiectelor realizate, Dan a acumulat experienta in sisteme informatice foarte variate incluzand sisteme de tip internet/ home/ mobile banking, sisteme de tip Core-Banking, sisteme de tip ERP, sisteme de raportare catre BNR, sisteme de tranzactionare, compensare si decontare, sisteme de management al fondurilor de investitii si de pensii. Dan a furnizat servicii IT pentru mai mult de 300 de companii din mai multe industrii, cum ar fi: industria financiar-bancara, asigurari, retail, industria producatoare si Oil&Gas.

Experienta lui Dan include si alte proiecte de consultanta, in care a fost implicat, cum ar fi: analiza cerintelor de afacere si definirea specificatiilor functionale pentru sisteme informatice, revizuiri post-dezvoltare ale unor sisteme informatice, elaborarea si revizuirea procedurilor operationale si de securitate IT pentru conformitatea cu standarde internationale precum ISO 27001 sau COBIT, dezvoltarea Planurilor de Continuitate a Afacerii si de Recuperare in Caz de Dezastru, elaborarea si revizuirea documentatiei necesare obtinerii acreditarii de furnizare a serviciilor de certificare, analiza si optimizarea proceselor de business etc.

Dan detine mai multe certificari cum ar fi:

- **CISA (Certified Information Systems Auditor);**
- **ISO 27001 Lead Auditor;**
- **ISO 27001 Lead Implementer;**
- **CIPM (Certified Information Privacy Manager);**
- CEH v10 (Certified Ethical Hacker);
- CompTIA Security+;
- Auditor de securitate cibernetica, atestat emis de catre DNSC;
- DPO (Data Protection Officer).

Teodor Lupan – Expert-cheie 3 – Expert testare securitate infrastructura retea

Teodor Lupan va actiona in cadrul echipei in calitate de Senior Expert testare a securitatii cibernetice.

Teodor are peste 18 ani de experienta in domeniul securitatii iinformatiilor care include, printre altele:

- Evaluare vulnerabilitati si teste de penetrare, incluzand teste de tip white box, grey box si black box,
- teste pentru identificarea si evaluarea vulnerabilitatilor de securitate folosind atat instrumente automatizate cat si investigare manuala;
- Audituri de securitate a sistemelor si solutiilor TIC bazate pe metodologii definite in standardele internationale de audit (COBIT si ISACA);
- Evaluarea stilului de programare si a eficientei designului aplicatiei din punctul de vedere al codului sursa
- Managementul incidentelor de securitate
- Analizele de securitate ale sistemelor si solutiilor TIC implementate;
- Evaluari de risc bazate pe standarde internationale;

Teodor detine Diploma de Master in Implementarea si Managementul Retelelor Informatice.

Teodor este certificat in:

- **Licensed Penetration Tester (LPT)**
- **Offensive Security Certified Professional (OSCP)**
- **Offensive Security Wireless Professional (OSWP)**
- **Certified Ethical Hacker (CEH)**
- Auditor de securitate cibernetica, atestat emis de catre CERT-RO
- Auditor Sef ISO 27001
- EC Council Security Analyst (ECSA)
- Global Industrial Certified Security Professional (GICSP)
- Introduction to Cyber Warfare and Operations Design (CSFI)

Ionut Georgescu – Expert-cheie 4 – Expert testare securitate sisteme informatice

Ionut Georgescu va lucra in cadrul proiectului ca Expert testare securitate sisteme informatice. Ionut detine o experienta vasta in domeniul securitatii IT si al administrarii sistemelor informatice acumulata in cei peste 18 ani de activitate in domeniul serviciilor IT. Experienta lui Ionut, include printre altele:

- Teste de penetrare de tip black box, grey box, white box;
- Audituri de securitate pentru aplicatii de tip Internet, Mobile si Phone Banking;
- Audituri de securitate pentru infrastructura SWIFT;
- Audituri de securitate pentru Sistemul Electronic de Plati (SEP);
- Revizuirea codului sursa;
- Implementarea standardelor de securitate (de ex. PCI);
- Instalarea si securizarea si administrarea sistemelor de tip Linux, Unix;
- Definirea arhitecturilor hardware si software pe platforma Linux si Unix;
- Dezvoltare de proceduri pentru securizarea sistemelor de tip Linux conform celor mai bune standarde in domeniu;
- Administrarea clusterelor VMware;
- Administrarea bazelor de date Oracle.

Ca parte a experientei sale, Ionut a acumulat vaste cunostinte in tehnologii si sisteme IT precum: Sisteme de operare Unix: HP-UX, SOLARIS, AIX; Linux: Redhat, Suse, Centos, Ubuntu; Programare: PL/SQL, Shell scripting, Perl, Python; Baze de date: SQL Server, Oracle 9i, 10g, 11g.

Ionut detine certificari precum:

- **CISSP (Certified Information Systems Security Professional);**
- **CEH7 (Certified Ethical Hacker);**
- **VMWare**
- **RHCE (Red Hat Certified Engineer - Red Hat Enterprise Linux 6);**
- **Oracle Database 10g: Administration I si Administration II;**
- CISM (Certified Information Security Manager;
- Auditor de securitate cibernetica, atestat emis de catre CERT-RO
- CompTIA PenTest+
- ECSA (Certified Security Analyst);
- QualysGuard - Vulnerability Management;
- ISO 27001 Auditor;

Oana Stoian - Expert-cheie 5 – Expert testare securitate sisteme informatice si infrastructurilor de tip WiFi

Oana Stoian este propusa in cadrul echipei in calitate de Expert testare securitate sisteme informatice si infrastructurilor de tip WiFi.

Oana detine o experienta de peste 8 ani in domeniul securitatii iinformatiilor care include:

- Evaluari ale vulnerabilitatii sistemelor IT si a infrastructurilor de retea;
- Teste de penetrare wireless
- Teste de penetrare retea si aplicatii web
- Analize ale riscurilor de securitate asupra vulnerabilitatilor identificate;
- Efectuarea testelor de regresie
- Testarea aplicatiilor POS inainte de implementare
- Certificarea aplicatiilor POS folosind instrumentele bancare specifice
- Evaluarea infrastructurilor critice

Oana detine un Master in Protectia Infrastructurilor Critice si este certificata:

- **Certified Ethical Hacker (CEH)**
- **Offensive Security Wireless Professional – OSWP**
- **Offensive Security Certified Professional – OSCP**
- CompTIA Security+
- Project Management

7 Referinte

Pentru a realiza auditul propus, am constituit o echipa cu experienta vasta in domeniul auditului IT. Pana in prezent, membrii acestei echipe au furnizat tipul acesta de servicii la peste 600 de clienti. Prezentam, in continuare, o selectie dintre cele mai reprezentative proiecte desfasurate si informatiile despre clienti:

- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Banca Nationala a Moldovei;**
- Analiza Sistemului Integrat de Gestionare a Cazurilor (ICMS) si identificarea oportunitatilor de imbunatatire, inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **World Bank, Republica Moldova – 2 proiecte distincte;**
- Audit de securitate IT pentru 18 sisteme inclusiv evaluarea vulnerabilitatilor de securitate, teste de penetrare pentru **Centrul de E-guvernare al Republicii Moldova**, Chisinau;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Ministerul de Justitie al Republicii Moldova** (subcontractant al Millennium DPI Partners pentru USAID - Open Justice Project, dezvoltarea noului sistem integrat de gestionare a cazurilor) ;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Ministerul de Justitie al Republicii Moldova (**subcontractant al **Checchi and Company Consulting**, dezvoltarea noului sistem integrat de gestionare a cazurilor)
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Moldova AgroindBank**, Chisinau;
- Audit de securitate IT pentru **BCR Chisinau**;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Banca Nationala a Romaniei**;
- Audit de securitate care a inclus evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru infrastructura IT si 35 aplicatii pentru **BCR S.A**.;
- Audit IT si teste de penetrare ale solutiilor de Internet Banking si Mobile Banking pentru **Garanti Bank** in conformitate cu Ordinul MCSI nr. 553/2019 (2 proiecte distincte);
- Audit IT si teste de penetrare ale solutiei de Internet Banking pentru **Banca Romaneasca** in conformitate cu Ordinul MCSI nr. 553/2019 (2 proiecte distincte);
- Audit IT in conformitate cu Ordinul MCSI nr. 553/2019 pentru **Orange Money IFN**

- Audit IT si teste de penetrare ale solutiilor de Internet/ Mobile Banking pentru **Credit Agricole Bank Romania** in conformitate cu Ordinul MCSI nr. 553/2019 (2 proiecte distincte);
- Audit IT si teste de penetrare ale solutiilor de Internet, Mobile si Phone Banking pentru **CEC Bank** in conformitate cu Ordinul MCSI nr. 553/2019 ;
- Audit IT si teste de penetrare ale solutiilor de Internet Banking si Mobile Banking in conformitate cu Ordinul MCSI nr. 553/2019 pentru **Techventures Bank**;
- Teste de penetrare ale solutiei de Online Onboarding pentru **Techventures Bank**;
- Audit IT si teste de penetrare ale solutiilor de Internet Banking si Mobile Banking in conformitate cu Ordinul MCSI nr. 553/2019 pentru **BRCI;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **BT Pensii**;
- Audit de securitate care a inclus evaluarea vulnerabilitatilor de securitate, teste de penetrare si teste de inginerie sociala pentru **BCR PENSII SAFPP S.A.**;
- Teste de penetrare si revizuire cod aplicatii pentru **Credit Europe Bank;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Libra Internet Bank** ;
- Evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Unicredit Consumer Financing SA;**
- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr. 362/2018 pentru **BCR SA;**
- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr. 362/2018 pentru **Banca Romaneasca;**
- Audit de securitate pentru conformitatea cu Legea NIS nr. 362/2018 pentru **First Bank;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Euro Finans AB Sweden** ;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Barwa Bank Qatar**;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **NMB Bank Tanzania**;
- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **BCR S.A.;**
- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **Banca Romaneasca S.A.;**

- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **CEC BANK S.A.;**
- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **Libra Bank.;**
- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **First Bank.;**
- Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022) pentru **Revolut Bank;**
- Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022) pentru **UniCredit Bank;**
- Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022) pentru **Credit Europe Bank;**
- Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022) pentru **Intesa Sanpaolo Romania;**
- Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022) pentru **UniCredit Consumer Financing IFN;**
- Audit IT pentru evaluarea conformitatii cu cerintele ANAF (Ordinul 146/2022) pentru **RCI Leasing IFN;**
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR, pentru **Banca Romaneasca** (2 proiecte distincte);
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR pentru **Libra Internet Bank**;
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR pentru **Garanti Bank**;
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR, pentru **IDEA Bank**;
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR pentru **CEC Bank**;
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR pentru **Intesa Sanpaolo Romania**;
- Audit al sistemelor de plati in conformitate cu prevederile Transfond si BNR pentru **Techventures Bank**;Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **KMG Rompetrol**
- Evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Regina Maria;**

- Audit IT si teste de penetrare pentru sistemele informatice din cadrul **Primariei Municipiului Buzau**;
- Servicii de securitate a informatiei si teste de penetrare pentru beneficiarii finali ai Bithat Solutions – **CJ Botosani si Ministerul Justitiei**;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Total Soft**;
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Computer Generated Solutions Romania** – 2 proiecte distincte. Asigurarea conformitatii cu cerintele PCI DSS (Standardul de securitate al cardurilor de plata);
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Agentia de Plati si Interventie pentru Agricultura (APIA) - 5 proiecte distincte;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Agentia pentru Finantarea Investitiilor Rurale (AFIR) – 3 proiecte distincte;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **EOS KSI;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Spearhead Systems LLC;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Erste Asset Management;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Inform Lykos;**
- Evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **BDO Romania;**
- Evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **UNIQA Asigurari;**
- Evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Contexpert Consulting SRL (2 proiecte distincte);**
- Evaluarea securitatii IT pentru platforma Yango a aplicatiei gazduite in cloud, inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Yandex LLC;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Ministerul Administratiei si Internelor, Departamentul pentru Evidenta Administrarii Personale si a Bazelor de Date;**
- Audit IT si teste de penetrare pentru **Alfatrust Certification;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **CERTDIGITAL - 2 proiecte distincte;**

- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **DotGov Solutions;**
- Audit IT si teste de penetrare pentru **Centrul de Calcul - 2 proiecte distincte;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Equity Invest;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Certinvest Pensii SAFPF (3 proiecte distincte);**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **SAI Certinvest;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate, teste de penetrare si teste de inginerie sociala pentru **ABC Asigurari Reasigurari;**
- Audit de securitate informatica inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Oficiul de Stat pentru Investitii si Marci (OSIM);**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate, teste de penetrare si teste de inginerie sociala pentru **SIF Banat Crisana;**
- Audit de securitate IT inclusiv evaluarea vulnerabilitatilor de securitate si teste de penetrare pentru **Tradeville Group;**
- Audit IT pentru Sistemul de Control al Miscarii Produselor Accizabile (EMCS) implementat de **Agentia Nationala de Administrare Fiscala**;
- Audit informatic si emiterea Certificatului de Conformitate a Securitatii Sistemului AEOI (Automatic Exchange of Information) implementat de **Agentia Nationala de Administrare Fiscala**;
- Audit de securitate pentru conformitatea Legea NIS nr. 362/2018 pentru **Farmexim;**
- Audit de securitate pentru conformitatea Legea NIS nr. 362/2018 pentru **Helpnet;**
- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr. 362/2018 pentru **Complexul Energetic Oltenia;**
- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr. 362/2018 pentru **Regia Autonoma „Administratia Canalului Navigabil Bega" Timis;**
- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr. 362/2018 pentru **Serviciul de Ambulanta Bucuresti Ilfov;**
- Audit de securitate pentru conformitatea Legea NIS nr. 362/2018 pentru **Tinmar Energy;**

- Audit de securitate pentru conformitatea Legea NIS nr. 362/2018 pentru **EDPR Romania;**

- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr. 362/2018 pentru **Antibiotice SA;**

- Audit de securitate si teste de penetrare pentru conformitatea cu Legea NIS nr.362/2018 pentru **Agentia Romana de Salvare a Vietii Omenesti pe Mare (ARSVOM);**

- Audit de securitate pentru conformitatea cu Legea NIS nr. 362/2018 pentru **Medical Express;**

- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **Trans Sped S.R.L.**;

- Audit IT pentru evaluarea conformitatii solutiei de identificare video la distanta pentru **Starbyte S.R.L.;**

- Audit IT pentru certificarea serviciilor de incredere conform Regulamentului (UE) Nr. 910/2014 pentru **Serviciul de Telecomunicatii Speciale**;

- Audit IT pentru certificarea serviciilor de incredere conform Regulamentului (UE) Nr. 910/2014 pentru **Centrul de Calcul S.A.**;

- Audit IT pentru certificarea serviciilor de incredere conform Regulamentului (UE) Nr. 910/2014 pentru **Alfatrust Certification S.A.**;

- Audit IT pentru obtinerea acreditarii MCSI pentru activitatea de furnizare a serviciilor de certificare conform Ordinului Ministrului nr. 473/ 09.06.2009 privind procedura de acordare, suspendare si retragere a deciziei de acreditare a furnizorilor de servicii de certificare, cu modificarile si completarile ulterioare pentru **Centrul de Calcul S.A.**

- Audit IT pentru obtinerea acreditarii MCSI pentru activitatea de furnizare a serviciilor de certificare conform Ordinului Ministrului nr. 473/ 09.06.2009 privind procedura de acordare, suspendare si retragere a deciziei de acreditare a furnizorilor de servicii de certificare, cu modificarile si completarile ulterioare pentru **Alfatrust Certification S.A.**

- Audit IT pentru verificarea indeplinirii conditiilor de autorizare a centrului de date conform cerintelor Ordinului MCSI nr. 489/15.06.2009 privind normele metodologice de autorizare a centrelor de date in cadrul **Telekom Romania Communications S.A.**

- Audit IT pentru verificarea indeplinirii conditiilor de autorizare a centrului de date conform cerintelor Ordinului MCSI nr. 489/15.06.2009 privind normele metodologice de autorizare a centrelor de date in cadrul **Orange Romania Communications S.A.**
- Audit IT in vederea reevaluarii indeplinirii cerintelor pentru certificare tehnica necesara pentru participarea la componentele Sistemului Electronic de Plati (ReGIS, SENT, SaFIR) pentru **Ministerul de Finante**;
- **Allianz Tiriac Asigurari** – Servicii de audit intern IT conform cerintelor Departamentului de Audit Intern;
- **Grupul Tradeville S.A.** - Audituri IT care au inclus: revizuiri ale controalelor generale IT, evaluarea vulnerabilitatilor de securitate si teste de penetrare externe si interne, audit de functionalitate a sistemelor informatice etc.
- **Altex Romania** – Servicii de consultanta IT ce au inclus: Analiza necesitatilor de acces ale angajatilor si dezvoltarea pe baza acestora a unor matrice de drepturi care respecta principiul segregarii responsabilitatilor precum si Dezvoltarea procedurilor operationale IT.

Peste 600 de alti clienti pentru care am prestat servicii similare.

8 Concluzii

Speram ca aceasta propunere indeplineste asteptarile Dumneavoastra. Va rugam sa nu ezitati sa ne contactati daca aveti intrebari legate de propunerea noastra sau pentru a obtine orice alte informatii de care aveti nevoie.

Aceasta propunere este valabila pana la data de 31 ianuarie 2023.