Grant Thornton

Agenția de Guvernare Electronică (AGE) – Servicii de testare de securitate pentru sisteme informaționale

Abordarea Noastră

Comentarii referitoare la Termenii de Referință

Înțelegerea Scopului și a Obiectivelor Specifice

Înainte de a merge la prezentarea metodologiei și strategiei noastre de implementare, am dori să abordăm câteva aspecte cheie și să introducem considerațiile noastre, precum și ipotezele care ne vor permite să abordăm mai bine și să aliniem propunerea noastră la Termenii de Referință (TOR).

Conform înțelegerii noastre, misiunea reprezintă o inițiativă strategică a Agenției de Guvernare Electronică (AGE) din Moldova pentru a consolida poziția de securitate a ecosistemului său digital în expansiune. În esența sa, obiectivul este de a achiziționa servicii specializate de testare și audit în domeniul securității cibernetice care depășesc evaluările tradiționale, asigurându-se că platformele critice precum EVO Integrated Government Electronic Services, EVO-Sign pentru identitate și semnătură mobilă și e-KYC pentru identificarea la distanță îndeplinesc cele mai înalte standarde de securitate, confidențialitate, integritate și disponibilitate. Aceste platforme nu sunt doar soluții tehnice; ele sunt instrumente transformatoare care redefinesc interacțiunea cetățean-stat, iar securitatea lor este fundamentală pentru susținerea încrederii publice și a rezilienței operaționale.

Obiectivele specifice ale serviciilor solicitate sunt multiple. Acestea includ identificarea și documentarea exhaustivă a vulnerabilităților în toate straturile de aplicații, infrastructură și cod sursă; simularea controlată a scenariilor de atac din lumea reală prin testarea penetrării; și verificarea conformității cu standardele internaționale, cum ar fi OWASP, ISO/IEC, NIST și e-IDAS. În plus, angajamentul își propune să ofere recomandări de remediere acționabile, să valideze eficacitatea măsurilor corective prin teste de urmărire și să integreze constatările în sistemele AGE de urmărire a erorilor pentru a asigura gestionarea completă a ciclului de viață al problemelor de securitate. Aceste obiective reflectă în mod colectiv o abordare proactivă a securității cibernetice, punând accentul atât pe măsurile preventive, cât și pe cele corective.

După ce am citit cu atenție Termenii de Referință, credem că scopul acestui angajament este cuprinzător: identificarea vulnerabilităților în straturile de aplicații, infrastructură și cod sursă; simularea scenariilor de atac din lumea reală prin testarea penetrării; și validarea conformității cu standardele internaționale și cele mai bune practici. Această abordare dublă—ofensivă și defensivă confirmă faptul că sistemele AGE nu sunt doar testate pentru puncte slabe, ci și comparate cu cadre recunoscute la nivel global, cum ar fi OWASP, ISO/IEC, NIST și e-IDAS. Alocarea pune accentul pe remedierea acționabilă, validarea de urmărire și integrarea cu sistemele AGE de urmărire a erorilor, creând un ciclu de viață complet al asigurării securității, mai degrabă decât un exercițiu unic.

Contextul și Importanța Strategică

Contextul acestei misiuni este modelat de două dinamici convergente: extinderea rapidă a serviciilor publice digitale din Moldova și sofisticarea crescândă a amenințărilor cibernetice. AGE lansează platforme de ultimă generație care gestionează acreditări de identitate sensibile, token-uri de autentificare și date biometrice, elemente care sunt foarte atractive pentru actorii rău intenționați. Aceste sisteme introduc suprafețe complexe de atac, inclusiv aplicații mobile, API-uri și fluxuri de lucru biometrice de verificare, care necesită tehnici avansate de validare a securității dincolo de scanarea convențională a vulnerabilităților.

La fel de importantă este dimensiunea de reglementare. Respectarea cadrelor europene, cum ar fi e-IDAS și standardele emergente pentru portofelele de identitate digitală, este esențială pentru interoperabilitate și încredere la nivel regional. Eșecul în atingerea conformității ar putea izola serviciile digitale din Moldova de inițiativele europene mai largi, limitând scalabilitatea și subminând credibilitatea. Astfel, această misiune nu este doar tehnică; este un imperativ strategic care stă la baza guvernanței digitale naționale, a încrederii cetățenilor și a integrării Moldovei în ecosistemul digital european.

Ipoteze Generale şi Consideraţii Cheie

Se presupune că sistemele AGE sunt operaționale sau în stadii avansate de dezvoltare, necesitând testarea în medii care reproduc îndeaproape condițiile de producție. Cooperarea deplină din partea echipelor tehnice și de afaceri ale AGE este esențială, inclusiv accesul în timp util la documentație, codul sursă și mediile de testare. Furnizorul trebuie să respecte protocoale stricte de confidențialitate și orientări etice, asigurându-se că activitățile de testare nu perturbă serviciile live sau compromit datele sensibile.

Considerațiile cheie includ diversitatea tehnologiilor din cadrul ecosistemului AGE, care necesită o abordare multi-cadru care combină orientările OWASP pentru aplicațiile web și mobile, standardele ISO/IEC pentru securitatea informațiilor și sistemele biometrice și metodologiile NIST pentru testarea structurată. Metodologia trebuie să fie adaptabilă, acoperind componentele web, mobile și backend, abordând în același timp riscurile unice, cum ar fi atacurile de prezentare, exploit-urile de reluare și scenariile biometrice de by-pass de legături în fluxurile de lucru e-KYC. Securitatea ciclului de viață este un alt aspect critic: vulnerabilitățile nu trebuie doar să fie identificate, ci și remediate și validate prin teste de urmărire, toate constatările fiind integrate în sistemele AGE de urmărire a erorilor pentru trasabilitate și responsabilitate.

Metodologia și Abordarea Tehnică

Abordarea tehnică este structurată și aliniată la cele mai bune practici internaționale. Începe cu o fază de planificare care definește domeniul de aplicare, obiectivele și regulile de implicare, urmată de o fază de evaluare care implică scanarea vulnerabilităților, testarea penetrării și auditurile de conformitate. Testarea va acoperi domenii critice, cum ar fi implementarea securizată, autentificarea, controlul accesului, securitatea criptografică, integritatea API și validarea logicii de afaceri. Pentru sistemele biometrice, testele specializate vor evalua rezistența la atac a prezentării, detectarea intensității și securitatea ciclului de viață al datelor biometrice. Faza finală se concentrează pe analiza, raportarea și testarea ulterioară pentru a confirma eficacitatea remedierii. Această metodologie structurată asigură nu numai o acoperire cuprinzătoare, ci și un transfer de cunoștințe către echipele AGE, consolidând rezistența la securitate pe termen lung.

Livrabilele și Cadrul de Raportare

Livrările sunt concepute pentru a oferi claritate și informații acționabile atât la nivel executiv, cât și la nivel tehnic. Rapoartele vor include rezumate executive concise pentru factorii de decizie și documentație tehnică detaliată pentru echipele de dezvoltare și securitate. Fiecare vulnerabilitate va fi clasificată utilizând CVSS v4.0, însoțită de dovezi ale conceptului și recomandări de remediere prioritare. Auditurile de conformitate vor include rezumate grafice și matrice detaliate care să cartografieze fiecare cerință în funcție de starea de conformitate. Integrarea cu sistemul AGE de urmărire a erorilor asigură urmărirea vulnerabilităților de la descoperire la închidere, creând un proces de remediere transparent și responsabil.

Importanța acestei misiuni se extinde dincolo de conformitatea tehnică. Într-o epocă în care încrederea digitală echivalează cu reziliența națională, securizarea platformelor de e-guvernare este o cerință fundamentală pentru transformarea digitală durabilă. Investind în teste și audituri de securitate structurate, AGE demonstrează o guvernare proactivă, protejează datele cetățenilor și poziționează Moldova ca participant credibil în inițiativele digitale regionale. Rezultatele acestui angajament nu

numai că vor atenua riscurile imediate, ci vor încorpora și o cultură a asigurării continue a securității, permițând Moldovei să navigheze cu încredere complexitatea unui viitor digital interconectat.

Particularități, Riscuri și Sensibilitatea Sistemelor

Sistemele luate în considerare prezintă caracteristici unice și sensibilitate sporită. EVO, ca platformă integrată pentru serviciile guvernamentale electronice, agregează mai multe funcționalități și fluxuri de date, făcându-l o țintă de mare valoare pentru atacatorii care caută perturbări sistemice. EVO-Sign introduce mecanisme criptografice pentru identitatea mobilă și semnăturile digitale, în care orice compromis ar putea invalida încrederea în tranzacțiile electronice și documentele juridice. Platforma e-KYC, care gestionează datele biometrice și verificarea identității la distanță, este deosebit de sensibilă datorită naturii ireversibile a identificatorilor biometrici și complexității reducerii riscurilor, cum ar fi atacurile de prezentare, exploatările de reluare și frauda bazată pe falsificare.

Aceste particularități amplifică riscurile asociate proiectului. Un atac de succes asupra oricăruia dintre aceste sisteme ar putea duce la furtul de identitate, fraudă pe scară largă sau chiar eșec sistemic al serviciilor publice. În plus, implicațiile de reglementare sunt semnificative: nerespectarea e-IDAS și a standardelor europene conexe ar putea pune în pericol interoperabilitatea produselor din Moldova în cadrul ecosistemului digital al UE, subminând obiectivele strategice pentru integrarea regională.

Viziune Generală pentru Realizarea Obiectivelor

Viziunea pentru atingerea acestor obiective se bazează pe o metodologie structurată, bazată pe standarde, care combină practicile de securitate ofensive și defensive. Abordarea începe cu o fază riguroasă de planificare, care definește domeniul de aplicare, regulile de implicare și criteriile de referință de conformitate. Aceasta este urmată de activități cuprinzătoare de evaluare, inclusiv scanarea vulnerabilităților, testarea penetrării în mai multe scenarii (black-box, gri-box, white-box) și audituri de securitate aliniate la cadrele internaționale. Testarea specializată pentru sistemele biometrice va aborda rezistența la atac de prezentare, detectarea duratei de viață și securitatea ciclului de viață al datelor biometrice.

Procesul finalizează cu raportarea detaliată şi transferul de cunoştinţe, asigurându-se că echipele tehnice şi de management a AGE înţeleg pe deplin riscurile şi atenuările recomandate. Integrarea cu sistemele AGE de urmărire a erorilor va permite monitorizarea și responsabilitatea continuă, transformând asigurarea securității dintr-un exercițiu unic într-o practică de guvernanță continuă. Această viziune pune accentul pe colaborare, transparență și adaptabilitate, asigurându-se că măsurile de securitate evoluează alături de progresele tehnologice și amenințările emergente.

Cele Mai Importante Provocări în Contextul Proiectului

Sunt anticipate mai multe provocări în executarea acestei misiuni. În primul rând, complexitatea și diversitatea ecosistemului digital al AGE necesită o abordare multi-cadru, care necesită expertiză în domenii de securitate web, mobile și biometrice. În al doilea rând, sensibilitatea datelor implicate, în special identificatorii biometrici—necesită măsuri stricte de confidențialitate și manipulare etică pe tot parcursul procesului de testare. În al treilea rând, natura dinamică a amenințărilor cibernetice înseamnă că metodologiile de testare trebuie să rămână agile, încorporând informații despre amenințări și modele de atac în evoluție. În cele din urmă, respectarea standardelor europene, menținând în același timp continuitatea operațională, reprezintă un echilibru delicat între rigoarea reglementărilor și fezabilitatea practică

Abordarea acestor provocări va necesita nu numai competență tehnică, ci și previziuni strategice, asigurându-se că angajamentul oferă rezultate durabile în materie de securitate care consolidează agenda de transformare digitală a produselor din Moldova.

Framework-uri

Complexitatea și sensibilitatea platformelor de eGovernment din Moldova - EVO, EVO-Sign și e-KYC - necesită o abordare de testare și audit de securitate bazată pe cadre recunoscute pe plan internațional. Aceste cadre oferă metodologii structurate, practici standardizate și tehnici dovedite pentru a asigura o acoperire cuprinzătoare a vulnerabilităților și a cerințelor de conformitate. Selecția lor nu este arbitrară; reflectă nevoia de rigoare, interoperabilitate și adaptabilitate într-un peisaj de amenințare care evoluează rapid.

În scopul acestui proiect, vom folosi setul de standarde acceptate la nivel internațional în domeniul securității cibernetice, guvernanței TIC, asigurării TIC și Securității Informației, cum ar fi:

- ISO/IEC 25010,
- ISO/IEC 27001,
- ISO/IEC 27005,
- NIST CSF 2.0,
- NIST SP 800-15,
- OWASP,
- eIDAS and EUDI Wallet Framework,
- MITRE ATT&CK Framework,
- Etc.

ISO/IEC 25000 Series (SQuaRE)

Seria ISO/IEC 25000, cunoscută sub numele de Sisteme și Cerințe de Calitate Software și Evaluare (SQuaRE), este concepută pentru a stabili un cadru cuprinzător pentru evaluarea calității software-ului. Spre deosebire de standardele pur orientate spre securitate, SQuaRE abordează mai multe caracteristici de calitate, inclusiv funcționalitatea, eficiența performanței, compatibilitatea, gradul de utilizare, fiabilitatea, mentenabilitatea și securitatea. Pentru această atribuire, relevanța sa constă în capacitatea de a evalua securitatea ca atribut de calitate într-un context mai larg de robustețe a sistemului și încrederea utilizatorilor.

Avantajul principal al ISO/IEC 25000 este perspectiva sa holistica. Prin încorporarea securității în cadrul modelului de calitate mai larg, se asigură că platformele AGE nu sunt doar sigure, ci și fiabile, ușor de utilizat și ușor de întreținut. Acest lucru este deosebit de important pentru sisteme precum EVO și EVO-Sign, care trebuie să ofere utilizatorilor experiențe fără probleme, menținând în același timp controale stricte de securitate. Pentru e-KYC, unde verificarea biometrică introduce fluxuri de lucru complexe, SQuaRE ajută la validarea faptului că mecanismele de securitate nu compromit gradul de utilizare sau performanța sistemului. Importanța sa în acest proiect provine din necesitatea de a echilibra securitatea tehnică cu excelența operațională, asigurându-se că serviciile digitale rămân accesibile și de încredere.

Framework-urile OWASP

Open Web Application Security Project (OWASP) oferă o suită de orientări și standarde adaptate pentru securitatea aplicațiilor web și mobile. Pentru această misiune, Ghidul de Testare a Securității Web (WSTG) și Standardul de Verificare a Securității Aplicațiilor Mobile (MASVS) sunt indispensabile. WSTG oferă o abordare sistematică pentru identificarea vulnerabilităților în aplicațiile web, acoperind domenii precum validarea intrărilor, autentificarea și gestionarea sesiunilor. MASVS, completat de Mobile Application Security Testing Guide (MASTG), asigură faptul că aplicațiile mobile precum EVO-Sign îndeplinesc cerințe stricte de securitate, abordând riscuri precum stocarea nesigură, criptografia slabă și utilizarea necorespunzătoare a platformei.

Avantajul OWASP constă în orientarea sa practică și acceptarea globală. Acesta oferă metodologii clare de testare, taxonomii de vulnerabilitate și strategii de remediere, făcându-l extrem de relevant pentru platformele care gestionează date sensibile de identitate și autentificare. Importanța sa în acest context provine din faptul că EVO și EVO-Sign sunt aplicații orientate către utilizatori, unde deficiențele în logică sau configurare ar putea duce la exploatarea pe scară largă.

Standardele ISO/IEC

Cadrul ISO/IEC oferă o perspectivă orientată spre guvernanță, asigurându-se că practicile de securitate sunt încorporate în procesele organizaționale. ISO/IEC 27001 si 27002 pun bazele sistemelor de management al securitatii informatiei, in timp ce ISO/IEC 27005 se concentreaza pe managementul riscului. Pentru sistemele biometrice precum e-KYC, ISO/IEC 30107 este esențial, deoarece definește standardele pentru detectarea atacurilor de prezentare și protecția datelor biometrice.

Avantajul standardelor ISO/IEC constă în abordarea lor holistică, combinând controalele tehnice cu guvernanța, gestionarea riscurilor și conformitatea. Acestea sunt esențiale pentru a se asigura că poziția de securitate a AGE se aliniază cu cele mai bune practici internaționale și cu așteptările în materie de reglementare. Importanța lor este amplificată de sensibilitatea datelor biometrice, care necesită securitatea ciclului de viață - de la captare și stocare la transmitere și ștergere.

NIST SP 800-115

Institutul Național de Standarde și Tehnologie (NIST) oferă un ghid tehnic pentru testarea securității prin SP 800-115, care prezintă cele mai bune practici pentru planificarea, executarea și documentarea evaluărilor de securitate. Acest cadru este deosebit de valoros pentru structurarea activităților de testare a penetrării, asigurând coerența și repetabilitatea între diferite sisteme și medii.

Avantajul NIST SP 800-115 constă în claritatea și adaptabilitatea sa. Acesta oferă îndrumări detaliate privind execuția testelor, raportarea și analiza riscurilor, făcându-l ideal pentru ecosisteme complexe precum EVO și EVO-Sign, unde trebuie evaluate mai multe componente și puncte de integrare. Importanța sa în acest proiect este legată de necesitatea unei abordări disciplinate, bazate pe dovezi, a identificării și exploatării vulnerabilităților.

eIDAS și EUDI Wallet Framework

Respectarea regulamentului eIDAS și a standardelor europene emergente pentru Portofelul EUDI nu este negociabilă pentru platformele care gestionează identitatea digitală și serviciile de încredere. Aceste cadre definesc cerințele privind interoperabilitatea, asigurarea încrederii și gestionarea sigură a identității în întreaga UE. Pentru EVO-Sign și EVO, respectarea acestor standarde garantează că serviciile digitale din Moldova rămân compatibile cu inițiativele regionale, consolidând atât încrederea tehnică, cât și cea juridică.

Avantajul acestor cadre constă în autoritatea lor de reglementare și în rolul lor în facilitarea serviciilor digitale transfrontaliere. Importanţa lor nu poate fi supraestimată: nerespectarea lor ar putea izola platformele din Moldova de ecosistemele europene, subminând obiectivele strategice pentru integrarea digitală.

Alte Framework-uri de Suport

Metodologiile suplimentare, cum ar fi MITRE ATT&CK, CIS Benchmarks și PTES (Penetration Testing Execution Standard) oferă îndrumări specializate pentru modelarea amenințărilor, întărirea sistemului și testarea structurată a penetrării. Aceste cadre îmbunătățesc profunzimea și precizia evaluărilor de securitate, asigurându-se că activitățile de testare reflectă scenariile de atac din lumea reală și cele mai bune practici din industrie.

Selectarea acestor cadre nu este doar o alegere tehnică; este o decizie strategică care stă la baza credibilității și rezilienței ecosistemului de eGovernment din Moldova. Fiecare cadru abordează o dimensiune distinctă a vulnerabilităților la nivel de securitate, guvernanță și conformitate, rigoare tehnică și aliniere la reglementare. Împreună, acestea formează o arhitectură cuprinzătoare de asigurare a securității care atenuează riscurile, protejează datele sensibile și consolidează încrederea publică în serviciile digitale.

Abordarea

Metodologia și abordarea noastră fac obiectul următoarelor ipoteze:

- Toate etapele din planul de lucru sunt executate fără întârzieri de la Departamentele/unitățile AGE de Tehnologia informației și securitatea informației
- “Pregătit de client” documentele justificative sunt furnizate conform solicitării și în timp util de către Departamentul/Unitatea de Securitate a Informației și Tehnologia Informației al AGE
- Livrarea în timp util a raportului final este supusă contribuțiilor și feedback-ului din partea părților interesate din proiect atribuite de AGE
- Grant Thornton (‘GT’) nu va lua decizii de management și /sau nu se va înscrie în numele AGE, precum și GT nu va oferi consultanță juridică pentru AGE

- Punerea în aplicare a lacunelor identificate și evidențiate în rapoartele de analiză a riscurilor, rapoartele de audit de securitate IT, precum și în rapoartele de testare a penetrării, dacă este cazul, va fi responsabilitatea exclusivă a AGE
- Domeniul nostru de aplicare a serviciilor din prezenta propunere este limitat la cerințele definite în Termenii de Referință. În cazul în care AGE solicită Grant Thornton să efectueze servicii suplimentare în afara domeniului de activitate definit, acest lucru va fi discutat și convenit în mod oficial cu AGE
- Ca parte a domeniului de activitate predefinit și în timpul atribuirii, Grant Thornton nu va efectua nicio modificare a sistemului (software sau hardware).

Pentru implementarea cu succes a misiunii (în ceea ce privește Termenii de Referință pentru răspuns imediat), considerăm că cooperarea și colaborarea cu echipele AGE de IT și de Securitatea Informatiei reprezintă principalele principii de succes care ne vor permite să obținem rezultatele necesare și să oferim cele mai bune servicii bazate pe experiența, cunoștințele și abilitățile noastre. În etapa de planificare și stabilire a domeniului de aplicare ne așteptăm să avem câteva întâlniri cu principalele părți interesate și să stabilim o listă exactă a omologilor și a relațiilor noastre de lucru cu aceștia, inclusiv întâlniri, date necesare etc. Din partea noastră stabilim o echipă cu distribuția clară a domeniului de activitate și a sarcinilor atribuite fiecărui membru al echipei.

Controlul Calității și Management-ul Riscurilor

Controlul Calității

În calitate de membru al Grant Thornton International, ne angajăm să furnizăm servicii profesionale care respectă cele mai înalte standarde de calitate și etică, așa cum sunt prescrise de standardele de independență CREST (https://www.crest-approved.org/), International Federation of Accountants (IFAC) și Codul de Etică pentru Contabili Profesioniști emise de International Ethics Standards Board for Accountants (IESBA). Ca parte a angajamentului nostru, am stabilit procese riguroase de verificare a relațiilor și de acceptare a clienților, care asigură conformitatea serviciilor pe care le oferim cu toate cerințele de reglementare locale și internaționale aplicabile, precum și cu standardele industriale aplicabile. Atingerea excelenței profesionale înseamnă acceptarea și păstrarea clienților care împărtășesc valorile de calitate și integritate ale Grant Thornton. Politica de Acceptare și Consultare a Misiunilor Consultative este concepută pentru a identifica și evalua acele misiuni de consiliere care ar putea prezenta un risc semnificativ pentru GTIL și firmele membre sau în cazul în care ar putea fi necesare resurse profesionale suplimentare din întreaga rețea de Grant Thornton pentru a asigura calitatea și excelența muncii. Această politică se aplică atribuirilor pentru clienții potențiali și existenți care îndeplinesc unul sau mai multe dintre criteriile definite, pentru care este necesară consultarea cu GTI și aprobarea prealabilă.

În timpul executării Proiectului, vom efectua un control al calității, care este o parte obligatorie a standardului nostru corporativ. Evaluarea activității desfășurate în cadrul serviciilor de testare și audit de securitate ale serviciilor de sisteme/produse ale Agenției de Guvernare Electronică este o parte integrantă a aplicării îngrijirii profesionale cuvenite. Înainte de a emite raportul final și de a lua în considerare feedback-ul diferitelor părți interesate din partea Clientului și a altor părți interesate, vom examina toate documentele finale pregătite și documentele de lucru detaliate în ceea ce privește politica internă de control al calității Grant Thornton. Responsabilitatea pentru un angajament se extinde la fiecare persoană care contribuie la rezultatul final; cu toate acestea, Partenerul de angajament este pe deplin responsabil pentru angajament. Recenzorii pentru angajamente de atestare, cum ar fi aceste servicii de consultanță, sunt efectuate de Coordonatorul Global de Audit, managerul de proiect Global LTA și Administratorul Global de Proiect. Aceștia vor revizui proiectul și rapoartele finale pentru a determina dacă acestea sunt conforme cu standardele profesionale, politicile și procedurile Grant Thornton, semnând numai după ce au fost satisfăcute toate comentariile elaborate în timpul acestei revizuiri au fost abordate, după revizuirile corespunzătoare ale documentelor de lucru, documentației de angajament completată și asigurându-se că este adecvat ca Grant Thornton să emită raportul. În plus, Partenerul de angajament se va asigura că sunt îndeplinite atât standardele Grant Thornton de control al calității, cât și obiectivele de implicare ale proiectului.

Independența și Riscul

Standardele etice acceptate la nivel internațional impun ca profesioniștii contabili din practica publică să fie independenți și să evite orice conflict de interese care le-ar putea afecta independența și imparțialitatea. Înainte de executarea contractului nostru, vom efectua o Verificare a Relației de Independență (IRC) în întreaga rețea Grant Thornton, determinând orice relații trecute sau curente între firmele membre Grant Thornton și entitățile din structura corporativă a potențialului client. Prin acest control ne asigurăm că firmele noastre membre nu furnizează în prezent sau nu au furnizat în trecut servicii potențialului client sau entităților sale conexe, ceea ce ar putea crea conflicte de interese semnificative, reprezentând o amenințare la adresa independenței noastre ca profesioniști contabili publici. Vom lucra cu dumneavoastră din timp în procesul de executare a contractului, pentru a obţine informaţiile necesare cu privire la structura corporativă şi pentru a efectua IRC rapid (în intervalul de timp de 4 zile lucrătoare de la primirea informaţiilor solicitate), eliminând astfel eventualele probleme de conformitate şi economisind timp preţios în stabilirea unei colaborări cu firma noastră.

În plus, așa cum este prevăzut de procedurile GTIL de acceptare a clienților , precum și de Politica Global Advisory Assignment Acceptance and Consultation, vom efectua anumite verificări de fond pentru a exclude orice alți factori care ar putea afecta capacitatea noastră de a furniza servicii cu excelență profesională.

Atingerea excelenței profesionale înseamnă acceptarea și păstrarea clienților care împărtășesc valorile de calitate și integritate ale Grant Thornton. Politica de Acceptare și Consultare a Misiunilor Consultative este concepută pentru a identifica și evalua acele misiuni de consiliere care ar putea prezenta un risc semnificativ pentru GTIL și firmele membre sau în cazul în care ar putea fi necesare resurse profesionale suplimentare din întreaga rețea de Grant Thornton pentru a asigura calitatea și excelența muncii. Această politică se aplică atribuirilor pentru clienții potențiali și existenți care îndeplinesc unul sau mai multe dintre criteriile definite, pentru care este necesară consultarea cu GTI și aprobarea prealabilă.

Vă vom informa în plus dacă serviciile propuse necesită o procedură de verificare GTIL și vom executa serviciile de consultanță propuse numai în urma parcurgerii procedurilor descrise mai sus, având în vedere că acestea nu au evidențiat nicio amenințare la adresa independenței noastre sau a altor factori care ne pot împiedica să derulăm angajamentul.

Management-ul Riscurilor

Cheia pentru un angajament de succes este planificarea și managementul atent. Cu toate acestea, în ciuda unei dezvoltări atente, toate proiectele prezintă un anumit nivel de risc. În plus, riscurile unice ale fiecărui proiect pot face dificilă transferarea lecțiilor învățate de la o etapă la alta. Considerăm că un proces continuu de gestionare a riscurilor este o modalitate de a răspunde riscurilor neașteptate ale proiectului.

Este important să se înțeleagă procesele comune de gestionare a riscurilor și strategiile de atenuare a riscurilor, astfel încât să se poată obține rezultate de succes ale proiectului. Procesul de gestionare a riscurilor ajută la planificarea și anticiparea riscurilor, în timp ce strategiile de atenuare oferă instrumente pentru a le face față dacă se întâmplă acest lucru. Procesul de gestionare a riscurilor sau ciclul de viață reprezintă o modalitate structurată de abordare a riscurilor care se pot întâmpla în anumite proiecte.

Pentru a gestiona riscul de implicare și pentru a ne asigura că obiectivele și realizările sunt atinse, vom folosi abordarea cuprinzătoare pentru a gestiona ciclul de viață al riscului în timpul implementării angajamentului.

- Identificarea riscurilor.
  - Primul pas pentru a obține informații despre riscurile potențiale este să știți ce sunt. Acestea pot fi probleme de logistică, disponibilitatea personalului necesar, accesul la sisteme etc
- Analiza impactului potentialului risc
  - În etapa de analiză a riscurilor, explorăm probabilitatea apariției fiecărui risc, precum și impactul potențial pe care fiecare risc îl va avea asupra angajamentului. Lista riscurilor identificate va include un registru de risc care reprezintă o diagramă pentru fiecare risc, urmată de informații precum nivelul de prioritate și planurile de atenuare.
- Atribuirea priorității riscurilor

- În această etapă, acordăm prioritate riscurilor utilizând probabilitatea și impactul fiecărui risc pentru a determina nivelurile lor de risc. Aceasta înseamnă să atribuiți fiecărui risc o prioritate ridicată, medie sau scăzută pe baza factorilor determinati. Evaluarea riscurilor oferă echipei GT șansa de a vedea unde să-și concentreze energia în atenuarea riscurilor

– Mitigarea riscurilor

  - Elaborarea unui plan pentru a atenua fiecare risc și înregistrarea acestor planuri în registrul de risc. Cele mai frecvente patru modalități de a atenua riscurile includ evitarea, acceptarea, reducerea și transferul. A decide ce abordare să folosim pentru fiecare risc este o știință exactă și trebuie să ne folosim judecata și expertiza pentru a determina care este cea mai bună.

Trebuie remarcat faptul că toate riscurile identificate vor fi comunicate echipei AGE pentru a actualiza situația și a conveni asupra posibilelor strategii de rezolvare și atenuare a problemelor identificate. Partenerul de Angajament va fi în permanență în contact cu echipa AGE cu privire la acest aspect și alte aspecte importante ale acestui proiect.

Metodologia

Management-ul Proiectului

În scopul implementării misiunii, Grant Thornton își va executa cadrul de Management al Proiectului. Cadrul valorifică cele mai bune practici de management al programelor, management de proiect și management al performanței oferite de disciplinele tradiționale de management și le integrează pentru a oferi o abordare fără sudură și pragmatică pentru obținerea succesului proiectului. Acest set de procese și instrumente se bazează pe principii acceptate pe scară largă, cum ar fi cele descrise în cadrul Proiectelor În Medii Controlate (PRINCE2) și Ghidul PMIGeamings PMBOK®, Standardul pentru Managementul Portofoliului și Modelul Organizațional de Management al Maturității Proiectului. Metodologia noastră cuprinde, de asemenea, cele mai bune practici învățate în proiectele executate în timp util, rentabil și previzibil. Acest cadru utilizează componente, procese și tehnici PRINCE2 și este augmentat din Ghidul PMBOK® și din procesul și tehnicile de bune practici Grant Thornton.

Pe baza analizei noastre a obiectivelor auditului, a domeniului de aplicare al auditului aferent și a setului de rezultate, împreună cu etapele stabilite în Termenii de Referință, vă sugerăm să aveți următoarele principii de management al proiectului aplicate pentru atingerea obiectivelor auditului:

1. Acționați simplu și practic. Aceasta include dezvoltarea unei viziuni și a unei structuri clare pentru audit și utilizarea consecventă a instrumentelor și tehnicilor simple care sunt ușor de înțeles de către toate părțile interesate ale angajamentului

2. Implicarea și comunicarea puternică a părților interesate. Angajamentul are mai multe părți interesate și, prin urmare, este esențial să asigurăm implicarea deplină a părților interesate și să asigurăm o bună comunicare pe parcursul întregului ciclu de gestionare a proiectelor.

3. Management de proiect puternic. Angajamentul are mai multe livrabile cheie care sunt interconectate cu fazele ulterioare ale proiectului. Prin urmare, este deosebit de important pentru acest angajament să menținem un control ferm al timpului, costurilor și calității și să gestionăm în mod activ riscurile de implicare.

Abordarea angajamentului va fi după cum urmează:

În special, activitățile prezentate mai jos se vor desfășura în cadrul fiecărei faze de angajament.

Înainte de începerea oricărei misiuni de audit, serviciile de testare și audit de securitate ale sistemelor/produselor Agenției de Guvernare Electronică ar trebui planificate într-un mod adecvat pentru îndeplinirea obiectivelor de asigurare. Planul va acționa ca un cadru pentru angajamentul de audit și va servi la abordarea obiectivelor auditului.

Ca parte a procesului de planificare, vom obține o bună înțelegere a mediului IT. Pentru a executa angajamentul de audit conform unei abordări standardizate și structurate, vom identifica cadre de control adecvate care ar putea fi utile pentru acest audit.

Credem că implementarea sarcinilor menționate în Termenii de Referință va fi mai eficientă dacă planul detaliat al proiectului, precum și programul de audit sunt pregătite și convenite cu AGE înainte de începerea activităților principale.

Abordarea Tehnică

Abordarea tehnică pentru această misiune este concepută pentru a asigura o asigurare cuprinzătoare a securității pentru platformele critice ale Agenției de Guvernare Electronică: EVO, EVO-Sign și e-KYC, printr-o metodologie structurată aliniată la cele mai bune practici internaționale. Această abordare integrează tehnici ofensive și defensive, verificări riguroase de conformitate și teste specializate pentru sistemele biometrice, asigurându-se că vulnerabilitățile nu sunt doar identificate, ci și remediate și validate. Metodologia combină cadre recunoscute la nivel global, cum ar fi OWASP, NIST SP 800-115, standardele ISO/IEC, eIDAS și ISO/IEC 30107, aplicate într-o manieră adaptată caracteristicilor unice ale fiecărui sistem.

Punerea în Aplicare a Standardelor și Framework-urilor

Pentru EVO, care servește ca o platformă integrată pentru serviciile electronice, OWASP Web Security Testing Guide (WSTG) va fi aplicat pentru a evalua securitatea aplicațiilor web în domenii critice, cum ar fi validarea intrărilor, gestionarea sesiunilor și autentificarea. Testarea va include verificarea manuală a vulnerabilităților OWASP Top 10, completată de instrumente de scanare automată. Pentru EVO-Sign, Standardul de Verificare a Securității Aplicațiilor Mobile OWASP (MASVS) și Ghidul de Testare a Securității Aplicațiilor Mobile (MASTG) vor ghida evaluările riscurilor specifice dispozitivelor mobile, inclusiv stocarea nesigură și deficiențele criptografice. Ambele platforme vor fi, de asemenea, evaluate în raport cu NIST SP 800-115 pentru testarea structurată a penetrării și ISO/IEC 27001 pentru alinierea guvernanței.

Pentru e-KYC, conformitatea cu ISO/IEC 30107 este primordială pentru validarea mecanismelor biometrice de detectare a atacurilor de prezentare. Testele vor simula încercări de spoofing 2D și 3D, atacuri bazate pe deepfake și exploit-uri de reluare, asigurându-se că procesele de detectare a livității și de potrivire biometrică sunt rezistente. În plus, fluxurile de lucru e-KYC vor fi evaluate pentru securitatea ciclului de viață, acoperind captarea, transmiterea, stocarea și ștergerea datelor, în conformitate cu ISO/IEC 27002 și cu principiile de confidențialitate.

Abordarea Pentru Fiecare Tip de Serviciu

1 **Testarea Vulnerabilității:**

TProcesul începe cu scanarea automată folosind instrumente de vârf din industrie, cum ar fi Nessus, Nexpose și NMAP, completate de verificarea manuală pentru a elimina falsurile pozitive și pentru a descoperi defectele logice. Testarea vulnerabilității va viza configurații greșite, componente depășite și practici de codificare nesigure, asigurând o acoperire exhaustivă a straturilor de aplicații și de infrastructură.

Testarea vulnerabilității va servi drept bază pentru identificarea punctelor slabe ale aplicațiilor, infrastructurii și straturilor de configurare. Procesul începe cu scanarea automată utilizând instrumente de vârf din industrie, cum ar fi Nessus și Nexpose, completate de soluții open-source precum Nmap pentru evaluări la nivel de rețea. Aceste instrumente vor fi configurate pentru a detecta vulnerabilități comune, configurații greșite și componente depășite, urmând Ghidul OWASP Web Security Testing Guide (WSTG) pentru EVO și MASVS pentru EVO-Sign.

Cu toate acestea, doar scanarea automată este insuficientă pentru sistemele de această complexitate. Verificarea manuală va fi efectuată pentru a elimina falsurile pozitive și pentru a descoperi defectele logice pe care instrumentele automate nu le pot detecta. Aceasta include testarea pentru gestionarea necorespunzătoare a sesiunilor, puncte finale API

nesigure și căi de escaladare a privilegiilor. Pentru e-KYC, testarea vulnerabilității se va extinde la fluxurile de lucru biometrice, asigurându-se că mecanismele de captare și transmitere a datelor sunt întărite împotriva atacurilor de interceptare și reluare. Rezultatul va fi o hartă cuprinzătoare a vulnerabilității, clasificată în funcție de severitate utilizând CVSS v4.0, care formează baza pentru testarea ulterioară a penetrării

2 Testarea Penetrării (Black Box, Gray Box, White Box)

Testarea penetrării va urma metodologia NIST SP 800-115, structurată în faze de colectare a informațiilor, enumerare, exploatare și post-exploatare. Testarea Black Box va simula atacurile externe fără cunoștințe prealabile, Gray Box va folosi accesul limitat autentificat, iar White Box va implica revizuirea completă a codului sursă și analiza arhitecturală. Tehnicile vor include cartografierea rețelei, fuzz-ul API, încercările de escaladare a privilegiilor și exploatarea defectelor logice de afaceri, asigurând scenarii realiste de atac.

Testarea penetrării va simula scenarii de atac din lumea reală pentru a valida rezistența platformelor AGE în condiții contradictorii. Metodologia va urma NIST SP 800-115, structurată în faze de recunoaștere, enumerare, exploatare și post-exploatare.

- Black Box Testing va replica atacurile externe fără cunoștințe prealabile, concentrându-se pe interfețele expuse public, API-uri și mecanisme de autentificare.
- Gray Box Testing va utiliza accesul limitat autentificat, simulând amenințările din interior sau conturile de utilizator compromise pentru a testa escaladarea privilegiilor și mișcarea laterală.
- White Box Testing va implica acces complet la codul sursă și documentația arhitecturală, permițând analiza profundă a defectelor logice, implementări criptografice și puncte de integrare.

Exercițiul de testare a penetrării este un exercițiu de securitate care utilizează hackeri etici, mai degrabă decât procese automatizate sau hackeri din lumea reală care încearcă să deterioreze și/sau să compromită sistemele informatice ale companiei. Testarea penetrării încearcă să exploateze punctele slabe sau vulnerabilitățile din sisteme, rețele, resurse umane sau active fizice pentru a testa eficacitatea controalelor de securitate. Un test de penetrare implică o echipă de profesioniști în domeniul securității care încearcă în mod activ să intre în rețeaua companiei dvs., exploatând punctele slabe și vulnerabilitățile din sistemele corporative.

Pentru a asigura un test de penetrare reușit, există mai multe activități și procese care trebuie luate în considerare dincolo de testarea în sine. Această secțiune oferă o metodologie de nivel înalt pentru aceste activități și este organizată de fazele tipice care apar în timpul unui test de penetrare:

- Pre-angajament,
- Angajament,
- Post-angajament.

Pre-angajament

Obiectivul acestei activități este de a stabili un cadru de gestionare a riscurilor care să țină AGE la curent cu progresul nostru și să ajute ambele părți să gestioneze în mod eficient riscurile asociate. În mod specific, am căuta să identificăm în mod clar ce este și ce nu este testat, să comunicăm punctele de contact din cadrul clientului și Grant Thornton și să programăm activități pentru a minimiza riscul pentru afacere, care include:

- Scoping,
- Regulile de Angajament,
- Criteriile de Sucess.

Această fază a inclus, de asemenea, stabilirea unui punct de contact de urgență și a unor căi de escaladare pentru a informa despre orice vulnerabilitate critică cu risc ridicat care a fost descoperită imediat sau pentru a raporta probleme asociate cu testarea, de exemplu, un sistem care cedează în mod neașteptat. Rezultatul fazei de pre-angajament a fost Regulamentul de angajament semnat (RoE) cu AGE.

Domeniul de aplicare al testelor de penetrare este definiția convenită a ceea ce va fi testat (și ce, în mod explicit nu va fi) și modul în care aceste elemente vor fi testate.

Testarea penetrării este o activitate în care o echipă de testare (Echipa Grant Thornton) încearcă să eludeze procesele și controalele de securitate ale unui sistem informatic. Pozând ca intruși neautorizați interni sau externi, echipa de testare încearcă să obțină acces privilegiat, să extragă informații și să demonstreze capacitatea de a manipula componentele sistemului țintă în moduri neautorizate dacă s-ar fi întâmplat în afara domeniului de aplicare al testului. Datorită naturii sensibile a testelor de penetrare, sunt necesare reguli specifice de angajare pentru a se asigura că testarea este efectuată într-un mod care minimizează impactul asupra operațiunilor, maximizând în același timp utilitatea rezultatelor testelor.

Pentru a stabili în mod clar domeniul de activitate și procedurile care vor fi și nu vor fi efectuate, prin definirea obiectivelor, a termenelor, a regulilor de testare și a punctelor de contact, Regulamentul de angajament (RoE) va fi semnat între părți. Scopul Regulamentului de angajament (RoE) este de a stabili procedurile și regulile de angajament pentru momentul în care testarea penetrării este efectuată împotriva componentelor sistemului AGE selectate. În conformitate cu Termenii de Referință, se vor efectua următoarele teste:

- teste efectuate din rețeaua externă a AGE
- teste efectuate din rețeaua internă a AGE
- evaluări ale vulnerabilității
- Teste de rezistență operațională:
  - simulări privind volumul tranzacțiilor,
  - simulări ale cedării sistemului și recuperarea acestuia
  - simulări ale atacurilor DoS/DDoS.

Înainte de a începe angajamentul de testare a penetrării, vom confirma domeniul de aplicare și obiectivele, vom nota orice modificări și ne vom asigura că întregul personal relevant este conștient de proces prin conferințe video la distanță cu personalul tehnic desemnat.

Trebuie remarcat faptul că testul de penetrare nu este o încercare necoordonată de a accesa o resursă neautorizată. Activitățile de testare a penetrării ar trebui coordonate și programate împreună cu personalul AGE. Cel puțin, unele dintre testele de penetrare solicitate vor înregistra alerte într-un Sistem de Detectare a Intruziunilor. În plus, unele teste au capacitatea de a provoca o întrerupere a echipamentelor sau sistemelor de rețea. Din acest motiv, managementul companiei și conștientizarea personalului sunt necesare în majoritatea cazurilor. Informații despre încercările de penetrare pot fi găsite în jurnalele sistemelor vizate sau pe IDS care trebuie descrise în documentul RoE și furnizate către AGE înainte de începerea testului de penetrare. Pașii care vor fi făcuți după ce testerul detectează un compromis anterior sau activ la sistemele testate vor fi descriși în secțiunea de manipulare a incidentelor din documentul RoE. Clasele de probleme vor fi ridicate cu AGE, iar termenele și formatul în care ar trebui ridicate problemele ar trebui descrise în secțiunea privind gestionarea incidentelor din documentul RoE.

Unul dintre cele mai importante aspecte ale testului de penetrare este comunicarea cu clientul. Cât de des interacționați cu clientul și modul în care îl abordați poate face o diferență uriașă în sentimentul lor de satisfacție. Mai jos este un ghid de comunicare care va ajuta la a face AGE să se simtă confortabil cu privire la activitățile de testare.

- Orice fel de comunicare cu alte persoane din cadrul AGE care nu sunt direct implicate în test și se referă la datele de testare este interzisă, cu excepția celor care vor fi atribuite direct de AGE
- Toate comunicările legate de anumite date de testare sau de testare cu echipa Grant Thornton vor fi efectuate electronic, cu metode de comunicare internă care acceptă criptarea datelor în tranzit (de ex. Sistem de e-mail corporativ),

- Toate punctele de contact pentru echipa Grant Thornton, personalul AGE adecvat și echipa de răspuns la incidente trebuie identificate și documentate în RoE. Dacă este cazul, ar trebui furnizate, de asemenea, autorizații de securitate sau detalii comparabile privind verificarea antecedentelor
- Detalii privind programul de testare, orele în care va avea loc testarea și informații precum testele critice și reperele vor fi descrise în documentul RoE
- Criterii pentru oprirea testării securității informațiilor ar trebui să fie furnizate, la fel ca și detaliile privind cursul de acțiune al echipei de testare Grant Thornton în cazul în care o procedură de testare are un impact negativ asupra rețelei sau în cazul unui atac advers asupra companiei în timp ce testarea este în curs de desfășurare
- Răspunsul AGE la incidente ar trebui să fie furnizate într-un format de referință rapidă
- Un proces de reinstalare a echipei de testare și reluarea testării ar trebui să fie, de asemenea, furnizat în documentul RoE
- documentul RoE va include informații despre adresele IP autorizate și neautorizate sau alți identificatori distinctivi, dacă este cazul, pentru componentele sistemului și pentru orice aplicații care urmează să fie testate.

Angajament: Testarea Penetrării

Timpul și efortul care trebuie depuse pentru sistemele care au vulnerabilități trebuie estimate în consecință. După efectuarea planificării și pregătirii necesare cu AGE, următorul pas este de a aduna cât mai multe informații despre sistemele vizate sau componentele sistemului, inclusiv orice vulnerabilități cunoscute. După determinarea vulnerabilităților care există în sisteme, următoarea etapă este identificarea țintelor potrivite pentru o încercare de penetrare.

În ceea ce privește vectorii de atac, se vor utiliza următoarele abordări:

- Testarea Externă – direcționat către servere/dispozitive vizibile extern ale soluției de plată instantanee (de ex. DNS, e-mail, servere web, routere etc.)
- Testare internă - orientată către servere/dispozitive vizibile intern ale soluției de plăți instant
- Teste de reziliență operaționale:
  - Simulari de volumele de tranzacții,
  - Simulari de cedarea și recuperarea sistemului,
  - Simulari de atacuri DoS/DDoS.

În timpul unui test de penetrare, echipa de pen testeri va primi câteva informații cu privire la resursele disponibile public ale sistemului de plată instantanee în ceea ce privește testarea penetrării externe și unele informații disponibile pe plan intern. Principalul beneficiu al acestei metode de testare este de a simula un atac cibernetic din lumea reală, prin care echipa de testeri își asumă rolul unui atacator neinformat din sediul AGE. În scopul testării penetrării interne, conexiunea securizată (IPSEC) va fi stabilită cu rețeaua internă izolată AGE pentru a simula atacul, având în vedere că potențialul atacator a intrat deja în perimetrul intern AGE.

Scopul evaluării interne și externe este de a verifica securitatea perimetrului extern/intern și a serviciilor disponibile public ale sistemului de plăți instantanee. Testele vor dezvălui dacă există posibilitatea de a dezvolta un atac asupra resurselor disponibile.

Trebuie remarcat faptul că tacticile OSINT (Open-Source Intelligence Gathering) vor fi utilizate pentru a extrage informații pertinente disponibile prin surse precum postări de locuri de muncă, profiluri de social media ale angajaților și asociații terțe afiliate. Odată ce inteligența a fost colectată, a fost folosită pentru a crea o tactică de testare a penetrării pentru acest angajament.

Atacul extern/intern va fi inițiat pentru a evalua sistemele de apărare perimetrală AGE, vectorii potențiali de atac și protecția activelor orientate spre exterior, precum și a activelor orientate spre interior. Testul va implica o evaluare

cuprinzătoare a suprafeței de atac externe și interne, inclusiv a infrastructurii rețelei externe/interne, a aplicațiilor web și a oricăror servicii accesibile publicului. Obiectivele principale au fost identificarea vectorilor potențiali de atac, a vulnerabilităților, a punctelor potențiale de intrare și evaluarea rezistenței globale a posturii de securitate a soluțiilor de plată instantanee.

Toate serviciile și aplicațiile web vor fi evaluate în conformitate cu Ghidul de testare OWASP V4.2 și includ următoarele subiecte:

- Injection,
- Broken Authentication and Session Management,
- Cross-Site Scripting (XSS),
- Broken Access Control,
- Security Misconfiguration,
- Sensitive Data Exposure,
- Insufficient Attack Protection,
- Cross-Site Request Forgery (CSRF),
- Using Components with Known Vulnerabilities,
- Under protected APIs.

Vom efectua diverse activități de scanare, enumerare și atac pentru a identifica posibilele zone slabe de implementare sau aplicație/serviciu în sine. Prin evaluarea aplicatiilor si serviciilor web pentru domeniile OWASP am efectuat in urma testelor OWASP.

În ceea ce privește componentele infrastructurii, se vor efectua următoarele testări:

- **Testarea Configuration and Deployment Management**
  - Test Network/Infrastructure Configuration (OTG-CONFIG-001)
  - Test Application Platform Configuration (OTG-CONFIG-002)
  - Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)
  - Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)
  - Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)
  - Test HTTP Methods (OTG-CONFIG-006)
  - Test HTTP Strict Transport Security (OTG-CONFIG-007)
  - Test RIA cross domain policy (OTG-CONFIG-008)
- **Testarea Identity Management**
  - Test Role Definitions (OTG-IDENT-001)
  - Test User Registration Process (OTG-IDENT-002)
  - Test Account Provisioning Process (OTG-IDENT-003)
  - Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)
  - Testing for Weak or unenforced username policy (OTG-IDENT-005)
- **Testarea Autentificării**
  - Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)

  - Testing for default credentials (OTG-AUTHN-002)
  - Testing for Weak lock out mechanism (OTG-AUTHN-003)
  - Testing for bypassing authentication schema (OTG-AUTHN-004)
  - Test remember password functionality (OTG-AUTHN-005)
  - Testing for Browser cache weakness (OTG-AUTHN-006)
  - Testing for Weak password policy (OTG-AUTHN-007)
  - Testing for Weak security question/answer (OTG-AUTHN-008)
  - Testing for weak password change or reset functionalities (OTG-AUTHN-009)
  - Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)
- **Testarea Autorizării**
  - Testing Directory traversal/file include (OTG-AUTHZ-001)
  - Testing for bypassing authorization schema (OTG-AUTHZ-002)
  - Testing for Privilege Escalation (OTG-AUTHZ-003)
  - Testing for Insecure Direct Object References (OTG-AUTHZ-004)
- **Testarea Session Management**
  - Testing for Bypassing Session Management Schema (OTG-SESS-001)
  - Testing for Cookies attributes (OTG-SESS-002)
  - Testing for Session Fixation (OTG-SESS-003)
  - Testing for Exposed Session Variables (OTG-SESS-004)
  - Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)
  - Testing for logout functionality (OTG-SESS-006)
  - Test Session Timeout (OTG-SESS-007)
  - Testing for Session puzzling (OTG-SESS-008)
- **Testarea Input Validation**
  - Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)
  - Testing for Stored Cross Site Scripting (OTG-INPVAL-002)
  - Testing for HTTP Verb Tampering (OTG-INPVAL-003)
  - Testing for HTTP Parameter pollution (OTG-INPVAL-004)
- **Testarea pentru SQL Injection (OTG-INPVAL-005)**
  - Oracle Testing
  - MySQL Testing
  - SQL Server Testing
  - Testing PostgreSQL (from OWASP BSP)
  - MS Access Testing
  - Testing for NoSQL injection

  - Testing for LDAP Injection (OTG-INPVAL-006)
  - Testing for ORM Injection (OTG-INPVAL-007)
  - Testing for XML Injection (OTG-INPVAL-008)
  - Testing for SSI Injection (OTG-INPVAL-009)
  - Testing for XPath Injection (OTG-INPVAL-010)
  - IMAP/SMTP Injection (OTG-INPVAL-011)
  - Testing for Code Injection (OTG-INPVAL-012)
  - Testing for Local File Inclusion
  - Testing for Remote File Inclusion
  - Testing for Command Injection (OTG-INPVAL-013)
  - Testing for Buffer overflow (OTG-INPVAL-014)
  - Testing for Heap overflow
  - Testing for Stack overflow
  - Testing for Format string
  - Testing for incubated vulnerabilities (OTG-INPVAL-015)
  - Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016
- **Testarea pentru Error Handling**
  - Analysis of Error Codes (OTG-ERR-001)
  - Analysis of Stack Traces (OTG-ERR-002)
- **Testarea pentru Weak Cryptography**
  - Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)
  - Testing for Padding Oracle (OTG-CRYPST-002)
  - Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

Un avantaj principal al unui test de penetrare white box este că raportarea oferă o evaluare mai concentrată și mai eficientă a posturii de securitate AGE a aplicațiilor și componentelor sistemului selectat.

În ceea ce privește testul de rezistență operațională, trebuie remarcat faptul că acesta va fi executat în cadrul angajamentului de testare a penetrării interne.

Post-angajament

După efectuarea angajamentului sau a testării, există activități pe care ambele părți ar trebui să le desfășoare.

- Curățarea mediului
  - Este important ca testerul să documenteze și să dezvăluie AGE orice modificări aduse mediului (așa cum este permis în Regulile de angajament) în timpul testului, incluzând, dar fără a se limita la:
    (1) Conturile care au fost create ca parte a evaluării fie de către entitate, fie de către tester: Grant Thornton va elimina apoi aceste conturi.
    (2) Instrumentele instalate de tester pe sistemele AGE (dacă există): aceste instrumente trebuie eliminate la sfârșitul testării.

Eliminarea conturilor și a instrumentelor de testare va asigura faptul că conturile sau instrumentele rămase nu au putut fi exploatate sau utilizate împotriva AGE.

3 **Revizuirea Codului de Securitate:**

Static Application Security Testing (SAST) va fi efectuată cu ajutorul instrumentelor SonarQube, combinate cu inspecția manuală a codului pentru a identifica vulnerabilitățile pe care instrumentele automate le pot pierde. Revizuirea se va concentra pe modele de codificare nesigure, validare necorespunzătoare a intrărilor și defecte de implementare criptografică, asigurând alinierea cu practicile de codificare sigure OWASP.

Revizuirea codului de securitate va combina Static Application Security Testing (SAST) cu inspecția manuală pentru a identifica vulnerabilitățile la nivelul codului sursă. Instrumentul automat SonarQube va fi folosit pentru a scana modele de codificare nesigure, validare de intrare necorespunzătoare, și puncte slabe criptografice. Revizuirea manuală va completa aceste instrumente, concentrându-se pe erorile de logică de afaceri, acreditările hardcoded și defectele de securitate API pe care scanările automate le ignoră adesea.

Pentru EVO și EVO-Sign, revizuirea codului va asigura conformitatea cu practicile de codificare securizate OWASP, în timp ce pentru e-KYC, o atenție deosebită va fi acordată rutinelor biometrice de gestionare a datelor, mecanismelor de criptare și logicii de manipulare a erorilor. Această abordare dublă garantează atât lățimea, cât și profunzimea, asigurându-se că vulnerabilitățile sunt detectate înainte de a putea fi exploatate.

4 **Auditul de securitate (Evaluarea GAP):**

Auditul de securitate va compara platformele AGE cu standardele recunoscute la nivel internațional, inclusiv eIDAS pentru servicii de încredere, OWASP MASVS pentru securitate mobilă și ISO/IEC 30107 pentru integritate biometrică. Procesul de audit va implica revizuiri detaliate ale configurației, analize arhitecturale și maparea conformității, producând o matrice care indică în mod clar conformitatea, conformitatea parțială sau neconformitatea pentru fiecare cerință.

Pentru EVO și EVO-Sign, auditurile vor valida respectarea cerințelor eIDAS pentru asigurarea identității și interoperabilitate, în timp ce pentru e-KYC, conformitatea cu ISO/IEC 30107 va confirma robustețea mecanismelor de detectare a atacurilor de prezentare. Auditul va include, de asemenea, repere CIS pentru întărirea sistemului și MITRE ATT&CK pentru modelarea amenințărilor, asigurându-se că platformele AGE sunt aliniate cu cele mai bune practici pentru rezistența împotriva amenințărilor avansate.

Abordarea specifică pentru e-KYC

Platforma e-KYC necesită teste specializate datorită dependenței sale de verificarea biometrică și datele sensibile de identitate. Detectarea atacurilor de prezentare (PAD) va fi evaluată utilizând atacuri foto de înaltă rezoluție, simulări 3D mask și videoclipuri deepfake pentru a îngreuna mecanismele de detectare a autenticității. Reluarea scenariilor de atac va testa integritatea sesiunii, în timp ce testele de falsificare a documentelor vor evalua capacitatea sistemului de a detecta documentele de identitate modificate digital. Încercările de bypass biometric vor simula procesele de înscriere frauduloase utilizând date de identitate și biometrice nepotrivite, asigurând o legătură strictă între document și verificarea biometrică.

Sumar

Această abordare tehnică este cuprinzătoare, combinând tehnici automate și manuale, strategii ofensive și defensive și audituri bazate pe conformitate. Utilizând cadre recunoscute la nivel global și adaptându-le la caracteristicile unice ale EVO, EVO-Sign și e-KYC, metodologia asigură identificarea vulnerabilităților, atenuarea riscurilor și asigurarea conformității fără a compromite continuitatea operațională. Integrarea testelor de urmărire și urmărirea erorilor asigură responsabilitatea și securitatea ciclului de viață, transformând acest angajament într-o piatră de temelie a rezistenței digitale a Moldovei.

Planul Proiectului

Gestionarea eficientă a proiectelor este esențială pentru menținerea controlului și transparenței. Comunicarea cu AGE va fi guvernată de un protocol structurat, care va include actualizări săptămânale ale progresului și escaladarea imediată a vulnerabilităților critice. În conformitate cu cerințele din Termenii de Referință, orice vulnerabilitate clasificată drept critică va declanșa o notificare în termen de 24 de ore, însoțită de orientări preliminare privind atenuarea.

Procedurile de gestionare a riscurilor vor aborda eventualele întreruperi ale serviciilor în timpul testării. Toate activitățile vor fi programate în timpul ferestrelor de întreținere predefinite, iar mecanismele de rezervă vor fi stabilite pentru a preveni întreruperile operaționale. Asigurarea calității va fi pusă în aplicare prin evaluări ale tuturor rezultatelor, aderarea la șabloane standardizate și validarea cadrelor internaționale înainte de depunere.

Executarea cu succes a acestei misiuni necesită un plan de proiect structurat și disciplinat care să asigure claritatea obiectivelor, alocarea eficientă a resurselor și aderarea la cele mai bune practici internaționale. Planul este organizat în trei etape principale:

1 Planificarea și Pre-Evaluarea,

2 Evaluarea și Testarea,

3 Analiza și Raportarea.

Fiecare dintre etape include activități definite, rezultate și mecanisme de management pentru a garanta calitatea și finalizarea la timp.

Etapa I: Planificarea și Pre-Evaluarea

Această etapă inițială stabilește fundamentul pentru toate activitățile ulterioare. Obiectivul său principal este de a defini domeniul de aplicare, normele de implicare și metodologiile pentru testare și audit. Activitățile vor include o întâlnire oficială de lansare cu părțile interesate din cadrul AGE pentru a alinia așteptările, a confirma obiectivele și a identifica punctele tehnice și de afaceri de contact. Va urma un exercițiu detaliat de delimitare, cartografierea tuturor sistemelor din perimetru: EVO, EVO-Sign și e-KYC și determinarea adâncimii testării necesare pentru fiecare.

Resursele alocate acestei etape vor include un manager de proiect, responsabil de coordonare și comunicare și consultanți de securitate principali, însărcinați cu dezvoltarea Planului de Testare și Audit (Scopul Lucrului). Acest plan va prezenta metodologii bazate pe cerințele de conformitate OWASP WSTG/MASVS, NIST SP 800-115, ISO/IEC 30107 și eIDAS. Rezultatul pentru această etapă va fi un Plan de Proiect cuprinzător și un Plan de Test și Audit, aprobat de AGE, asigurându-se că toate părțile interesate au o foaie de parcurs clară înainte de începerea executării.

Activități Cheie

- Organizarea de kick-off cu toate părțile implicate
- Definiție clară a Perimetrului (scoping) și Obiectivelor
- Stabilirea regulilor de angajament, inclusiv a perioadelor de timp pentru testare și Proceduri de Escaladare
- Definirea Scenariilor Testare și/sau Standarde care vor fi utilizate pentru fiecare dintre cele trei Sisteme
- Identificarea persoanelor de contact tehnic si de afaceri
- Obținerea permiselor Scrieri Obligatorii pentru Teste de Conduită.

Livrabile Cheie

- Planul de proiect,

– Planulde Test și Audit (Scopul Lucrului), inclusiv scenariile, metodologiile și instrumentele), aprobate de EGM.

Cronologia Proiectului (durata)

Până la 2 (două) săptămâni.

Etapa II: Evaluarea și Testarea

A doua etapă reprezintă nucleul angajamentului, pe parcursul acestei etape se efectuează evaluări practice de securitate. Activitățile vor include scanarea vulnerabilităților utilizând instrumente automate, cum ar fi Nessus, Burp Suite și OWASP ZAP, completate de verificarea manuală pentru a identifica defectele logice și a elimina falsurile pozitive. Va urma testarea penetrării structurată în conformitate cu orientările NIST SP 800-115 și executată în trei moduri: Black Box, simulând atacuri externe; Gray Box, utilizând accesul autentificat limitat; și White Box, care implică revizuirea completă a codului sursă și analiza arhitecturală.

Revizuirea codului de securitate va fi efectuată utilizând SonarQube, combinată cu inspecția manuală pentru vulnerabilitățile logicii de afaceri. Pentru e-KYC, testele specializate vor valida securitatea biometrică, inclusiv detectarea atacurilor de prezentare (PAD), securitatea ciclului de viață al datelor biometrice și scenariile de bypass. Resursele pentru această etapă vor include specialiști în teste de penetrare, specialiști în revizuirea codurilor și experți în securitate biometrică, susținuți de o asigurare dedicată a calității care să conducă la monitorizarea respectării standardelor.

Activități Cheie

Domeniile minime de testare a securității ar trebui să acopere, fără a se limita la, următoarele domenii:

– Configurarea și gestionarea implementării sigure,
– Managementul identificării și autentificării,
– Controlul Accesului,
– Validarea datelor de intrare,
– Error and log management,
– Securitatea Criptografică,
– Testarea business logic,
– Securitatea la nivel de client,
– Testarea API,
– alte domenii, în conformitate cu cadrul de testare stabilit.

În cazul auditului de securitate (Evaluarea GAP), activitatea va consta în verificarea sistematică a controalelor de securitate ale aplicației conform standardului de referință stabilit în etapa de planificare. Pentru fiecare cerință a standardului, arhitectura, configurația și, dacă este necesar, codul sursă vor fi analizate pentru a determina gradul de conformitate.

Livrabile Cheie

– Rapoarte intermediare interimare (la cerere), notificări în timp real (în termen de 24 de ore) pentru vulnerabilități cu severitate critică.

Cronologia Proiectului (durata)

Până la 7 (șapte) săptămâni.

Etapa III: Analiza și Raportarea

Etapa finală se concentrează pe consolidarea constatărilor, validarea eforturilor de remediere și transferul de cunoștințe către echipele AGE. Activitățile vor include clasificarea vulnerabilităților utilizând CVSS v4.0, elaborarea rapoartelor tehnice detaliate și pregătirea rezumatelor executive pentru factorii de decizie. Testarea ulterioară va fi efectuată după remedierea pentru a confirma închiderea vulnerabilităților. Rapoartele vor fi structurate astfel încât să ofere claritate atât la nivel strategic, cât și la nivel tehnic, inclusiv matrice de conformitate pentru auditurile efectuate împotriva eIDAS, MASVS și ISO/IEC 30107.

Resursele alocate acestei etape vor include specialiști în raportare, responsabili de redactarea documentației cuprinzătoare și conducători tehnici, care vor valida constatările și vor oferi clarificări în timpul sesiunilor de prezentare. Integrarea cu sistemul AGE de urmărire a erorilor va asigura trasabilitatea și responsabilitatea pe tot parcursul ciclului de viață al remedierii.

Activități Cheie

- Analiza Referințelor și validarea tuturor rezultatelor obținute,
- Clasificarea vulnerabilităților Identificate utilizând un sistem standardizat (CVSS v4.0)
- Elaborarea raportului detaliat,
- Prezentarea rezultatelor către Echipele Tehnice și Management-ul AGE
- Acordarea de Suport și Clarificări pentru o înțelegere deplină a riscurilor.

Testarea Follow-up

După ce echipa de dezvoltare a AGE implementează măsuri de remediere, vom efectua un test de follow-up pentru a valida corectitudinea și eficacitatea acestora și pentru a confirma vulnerabilitățile de închidere

Livrabile Cheie

- Rapoarte de testare și analiză cu recomandări detaliate
- Prezentarea rezultatelor către Echipele Tehnice și Management-ul AGE
- Rapoarte de Follow-up.

Cronologia Proiectului (durata)

Până la 3 (trei) săptămâni.

Planul de proiect propus combină metodologia structurată, protocoalele de comunicare clare și gestionarea robustă a riscurilor pentru a oferi un program cuprinzător de asigurare a securității. Prin alinierea la standardele internaționale și integrarea practicilor de securitate a ciclului de viață, planul nu numai că abordează vulnerabilitățile imediate, ci și stabilește o bază pentru îmbunătățirea continuă, consolidând rezistența digitală a Moldovei.

Programul de Implementare

Programul de implementare se va întinde pe aproximativ 12 săptămâni, distribuite în cele trei etape:

1 Săptămânile 1–3: Planificarea și Pre-Evaluarea, inclusiv kick-off, scoping, și aprobarea Planului Test și Audit.

2 Săptămânile 4–9: Evaluarea și Testarea. care acoperă evaluările vulnerabilității, testarea penetrării, revizuirile de cod și testele biometrice specifice pentru e-KYC.

3 Săptămânile 10–12: Analiza și Raportarea, inclusiv pregătirea rapoartelor finale, sumarelor executive, prezentărilor, și testării follow-up.

Această cronologie asigură că toate sistemele, cum ar fi EVO, EVO-Sign și e-KYC, sunt evaluate temeinic fără a compromite continuitatea operațională.