Oferta tehnică

Serviciile de audit de securitate IT pentru soluția de plăți instant oferite de echipa FORT vor include:

- Analiza de riscuri de securitate aferenta soluției de plăți instant;
- Servicii de audit a securității soluției de plăți instant, inclusiv testarea controalelor de securitate implementate.

Rezultatul acestor activitati va fi asigurarea unei gestionari eficiente a riscurilor TIC și gestiunea eficientă a atacurilor cibernetice, precum si de a oferi o analiza a comportamentul sistemelor informatice în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în cadrul soluției de plăți instant.

Analiza de riscuri de securitate aferenta soluției de plăți instant va evalua riscurile operaționale și de securitate asocitate soluției de plăți instant.

Auditul securității va presupune formarea concluziilor relevante privind suficienţa şi eficienţa măsurilor de securitate implementate aferente utilizării soluției de plăți instant. Se vor simula valabilitatea contoalelor de securitate implementate aferente soluției de plăți instant prin exploatarea vulnerabilităților existente și cunoscute într-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența că acestea vor fi efectuate într-un mod etic, cu permisiunea Beneficiarului. Procesul va implica o analiză activă a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvată și din breșe cunoscute sau necunoscute, hardware și software.

A. Analiza de riscuri

Analiza de riscuri va fi efectuată conform celor mai bune practici în domeniu (ISO, NIST, COSO ERM).

Analiza de riscuri va identifica, evalua și prioritiza riscurile identificate și va conține:

- descrierea riscurilor identificate ce ar putea compromite confidențialitatea, autenticitatea și integritatea datelor aferente utilizării soluției de plăți instant și nonrepudierea tranzacțiilor;
- impactul în cazul materializării riscurilor identificate;
- descrierea măsurilor de control implementate pentru diminuarea impactului, clasificate după modul de organizare (tehnice, organizatorice, normative) și după modul de acțiune (preventive, detective, corective);
- riscurile reziduale (care rămîn după implementarea măsurilor de control), sau reevaluarea acestora cu aplicarea măsurilor de control adiționale pentru diminuarea impactului acestora pînă la un nivel acceptabil.

Domeniul de aplicare a analizei de riscuri va acoperi:

- Infrastructura IT;
- Aplicația soft;
- Mediul operațional;
- Riscuri de integrare.

In procesul de identificare a riscurilor, echipa FORT va:

- Identifica vulnerabilitatile tehnice și organizaționale asociate soluției de plăți instant;
- Evalua riscurile externe (atacuri cibernetice, amenințări naturale sau de mediu);
- Identifica riscurile umane;
- Identifica riscurile asociate furnizorilor de servicii.

METODOLOGIA DE ANALIZA A RISCURILOR DE SECURITATE IT

Metodologia de analiza a riscurilor adoptata este mixta (cantitativa-calitativa), adica evaluarea se bazeaza pe date matematice cuantificate si pe o evaluare calitativa (care pondereaza informatiile colectate) luand in considerare la

rezumarea rezultatelor analizei de risc efectele fiecarui proces/amenintare asupra elementului de sistem si resurselor in ansamblu.

Pentru realizarea cu succes a analizei de risc se va realiza o matrice RACI, pentru a defini sarcinile si responsabilitatile, care va include persoanele responsabile pentru fiecare subsarcina, aprobatorul si persoanele care contribuie si care urmeaza sa fie informate pentru implementarea sarcinilor.

Modelul propus pentru Matricea RACI are urmatoarea structura:

Etapa	**Departament Securitate IT**	**Departament Solutii IT**	**Data owner**	**Upper Management**	**Departament Risc Operational**	**Echipa IT (planning, arhitectura etc), daca este diferita de Departamentul Solutii IT**
Analiza de risc	R/A		R/C	I	C	
Definirea sistemelor de informatii	R/A	R/C	R/C		C	C
Identificarea riscurilor	R/A	R	C		C	R
Evaluarea riscurilor	R/A	C	C		C	
Diminuarea riscurilor	R	R/A	R/C		C	C
Monitorizarea riscurilor	R/A	C	I/C	I	C	C
Planul de actiune	R	R	R/A	I	C	R

Unde:

- R = Responsible (responsabil)
- A = Accountable (raspunzator)
- C = Consulted (consultat)
- I = Informed (informat)

In baza discutiei preliminare cu reprezentantii bancii, se va actualiza matricea RACI astfel incat sa reflecte departamentele relevante din structura BNM.

Metodologia ce urmeaza a fi utilizata pentru analiza riscurilor poate fi impartita in 5 procese principale, dupa cum urmeaza:

1. Stabilirea contextului
2. Modelarea contextului
3. Evaluarea si tratarea riscului
4. Documentarea analizei de risc
5. Implementare si monitorizare

1. Stabilirea contextului

1.1.Considerarea proceselor de afaceri

- Pe parcursul Analizei de risc, in vederea evaluarii riscurilor de securitate IT specifice institutiei care decurg din utilizarea tehnologiei informatiei aplicate de Banca, este necesar sa se tina seama de principalele procese de afaceri ale Bancii (pe baza criticitatii acestora) si de resursele IT implicate in aceste procese. Se vor lua in considerare procesele de afaceri si seturile de date/date aferente acestora, procesele critice de

afaceri fiind determinate pe baza lor in cadrul proceselor de management al continuitatii activitatii Bancii, atunci cand este elaborata analiza impactului asupra afacerii (BIA). La momentul colectarii informatiilor de baza pentru analiza riscului de securitate IT trebuie facuta o analiza de impact a afacerii.

1.2. Elementele si resursele sistemului

- Identificarea elementelor de sistem si a resurselor care servesc ca baza pentru analiza generala a riscului de securitate IT pentru intreaga banca trebuie sa se bazeze pe procese critice de afaceri si trebuie luate in considerare toate elementele de sistem afectate de aceste procese, precum si resursele necesare functionarii acestora. Lista de elemente de sistem trebuie completata cu elementele sistemelor de securitate IT.
- Analiza de risc care trebuie efectuata pe un anumit sistem sau mediu de sistem se bazeaza pe elementele sistemului/mediului de sistem in cauza.
- Numarul de procese critice de afaceri si numarul de seturi de date afectate de elementele individuale ale sistemului trebuie luate in considerare in lista de elemente de sistem stabilita in acest fel.

1.3. Amenintarile

- Amenintarile relevante pentru Banca trebuie identificate in scopul identificarii vulnerabilitatilor de securitate IT ale elementelor de sistem si resurse care deservesc procesele critice pentru afaceri. Suma tuturor amenintarilor reprezinta catalogul de amenintari; acesta trebuie construit in conformitate cu standardele ISO 27002 si ISO 27005.
- Catalogul de amenintari trebuie actualizat inainte de identificarea riscurilor, iar amenintarile care nu mai afecteaza Banca sunt eliminate, in timp ce noile amenintari care nu existau anterior sau nu erau aplicabile, dar erau deja relevante pentru Banca la momentul producerii analizei, sunt adaugate.
- Pentru ca Banca sa poata identifica si evalua pe deplin riscurile de securitate ale elementelor si resurselor sistemului informatic cu o atentie rezonabila, catalogul de amenintari trebuie sa acopere toate domeniile legate de securitatea IT (ex. management, planificare, dezvoltare, achizitii, operare etc) .

2. Modelarea contextului

2.1. Definirea clasificarii de securitate a sistemului (elementelor) IT

Informatiile de referinta sunt colectate ca pas pregatitor pentru implementarea analizei de risc. Pe parcursul implementarii acestui proces de analiza, pe baza registrului de dispozitive informatice al Bancii, se desfasoara mai multe etape elementare ale sarcinii de clasificare, dupa cum urmeaza:

- identificarea datelor (originale) gestionate de sistemul (elementul) IT dat,
- identificarea proprietarului datelor datelor (originale) gestionate de sistemul (elementul) IT dat,
- identificarea proprietarului sistemului (elementului)/sistemului IT in cauza,
- clasificarea sistemului (elementului) IT in clasa de securitate aplicata de Banca.

2.2. Identificarea tipurilor de amenintari (surse) si a efectelor acestora

- Urmatorul pas in analiza riscului trebuie sa fie identificarea amenintarilor potentiale (care afecteaza Banca in ansamblu in cazul unei analize complete a riscului Bancii si care afecteaza mediul (mediile) specific(e)) in cazul unui mediu specific in functie de domeniul de aplicare al evaluarii. Elementele care afecteaza Banca in ansamblu, precum dezastre naturale, ar trebui grupate in functie de principalele amenintari (de exemplu, amenintari pentru mediu, amenintari la adresa cladirii etc).
- In stabilirea principalelor grupuri de amenintari/ amenintari elementare trebuie avut in vedere in primul rand specificul mediului bancar; catalogul amenintarilor este elaborat in consecinta. Mediul de reglementare si standardele din industrie pot defini alte categorii decat cele descrise in catalogul de amenintari, de-a lungul carora catalogul actual de amenintari poate fi rearanjat. Cu toate acestea, metodologia folosita trebuie sa fie logica, transparenta si usor de aplicat. Daca pot aparea forme accidentale si deliberate ale unei amenintari, acestea pot fi prezentate ca amenintari elementare individuale. Catalogul de amenintari are o structura flexibila, ceea ce inseamna ca compozitia sa poate fi

modificata si actualizata in mod continuu in viitor prin adaptarea acestuia la mediul si infrastructura bancara.

- Amenintarile elementare de obicei nu afecteaza toate sistemele IT/elementele sistemului sau resursele, dar impactul unei amenintari elementare asupra securitatii informatiilor sau asupra mediului de control aplicabil Bancii in ansamblu este aproape acelasi, asa ca este recomandabil sa fie analizate intr-un mod uniform.

2.3. Identificarea capabilitatilor si oportunitatilor (surse ale riscului)

Amenintarile elementare la adresa resurselor, sistemelor/elementelor de sistem si elementelor de infrastructura ale Bancii trebuie evaluate dupa cum urmeaza:

- din punct de vedere al securitatii informatiilor, si a elementele de baza (confidentialitate, integritate si disponibilitate)asupra carora au impact,
- care este probabilitatea ca amenintarea elementara sa apara,
- daca exista o activitate de control sau un control suplimentar de securitate integrat in proces care reduce probabilitatea sau impactul amenintarii elementare.

Dupa cum este descris mai sus, trebuie definita o lista de amenintari (prin crearea catalogului de amenintari), care descrie importanta amenintarilor, probabilitatea aparitiei amenintarilor si impactul controalelor care reduc aparitia amenintarii (eficacitatea masurilor de protectie).

Catalogul de amenintari trebuie sa cuprinda si detalieze urmatoarele:

- Identificarea amenintarilor relevante (doar acele amenintari care au sau pot avea un impact relevant asupra Bancii).
- Criteriile pe care o amenintare le afecteaza:
  - Confidentialitatea (C),
  - Integritatea (I),
  - Disponibilitatea (A).
- Probabilitatea ca fiecare amenintare sa apara.
- Eficacitatea masurilor de protectie pentru a atenua impactul fiecarei amenintari.

2.4. Sarcini legate de catalogul de amenintari:

- Departament Securitate IT este responsabil de actualizarea si intocmirea catalogului de amenintari .
- Departament Securitate IT este responsabil de evaluarea generala a impactului C/I/A al amenintarilor.
- Clasificarea de securitate este determinata de proprietarii sistemului (elementelor) si aprobata de catre Departament Securitate IT, iar clasificarea C/I/A a sistemelor/elementelor sistemului este inclusa in acest document.
- Persoana responsabila de sistem (elemente) trebuie sa faca obiectul investigatiei (operator, administrator) si contribuie la identificarea amenintarilor relevante la adresa sistemului (elementului) pe care il gestioneaza.

Catalogul amenintarilor este revizuit si actualizat anual pe baza amenintarilor relevante in prezent la adresa Bancii si a valorilor estimate ale acestora C/I/A, probabilitatile de aparitie si impactul amenintarii. Catalogul amenintarilor este actualizat in cursul revizuirii anuale si este disponibil persoanelor implicate in procesul de analiza a riscurilor.

2.5. Cuantificarea importantei amenintarii

Pentru fiecare element, Confidentialitate, Integritate, Disponibilitate, se va realiza o analiza a impactului si se vor incadra in categorii de Nivel de risc de la 0 la 4, unde 0 – impact inexistent (criteriul nu este relevant) si 4 – impact puternic si se va analiza rezultatul obtinut, actualizand analiza de riscuri pentru fiecare categorie si nivel de impact.

2.6. Cuantificarea existentei probabilitatii

Pentru stabilirea probabilitatii, se va utiliza o scara de la 0 la 4, unde 0 - Amenintarea nu poate fi exploatata si 4 - Foarte probabil: usor de executat, necesita o investitie minima de cunostinte sau resurse.

2.7 Cuantificarea eficacitatii masurilor de protectie (optiuni) pentru atenuarea impactului amenintarilor

- Analiza riscului trebuie sa examineze „rezistenta" Bancii la amenintari, daca Banca este deja pregatita pentru aparitia amenintarii si a luat contramasurile necesare.

3. Evaluarea si tratarea riscului

In cursul evaluarii riscului, este considerata o vulnerabilitate daca o amenintare poate fi exploatata intr-o oarecare masura (oportunitate), daunand astfel Bancii, amenintarea devenind relevanta pentru elementul specific al sistemului.

Pe parcursul efectuarii analizei de vulnerabilitate, resursele, elementele de sistem si elementele de infrastructura ale Bancii trebuie evaluate pe baza efectelor pe care le poate avea incalcarea confidentialitatii, integritatii si disponibilitatii. Rezultatul evaluarii este influentat si de existenta (indeplinirea) cerintelor pentru principiile generale de securitate pentru fiecare nivel de securitate. De asemenea, trebuie evaluat impactul riscurilor specifice ale amenintarilor asupra elementului sau resursa/sistem/infrastructura.

In cursul procesului de analiza a riscurilor, se utilizeaza urmatoarele metode pentru a determina „prezenta" vulnerabilitatii:

- studiul documentatiei disponibile (descrierea producatorului, planul sistemului, planul de implementare, raportul de audit, securitatea informatiilor/materiale tehnice etc.),
- interviu personal sau interviu auto-raportat cu utilizatorii de operare/intretinere a sistemelor/elementelor sistemului.

3.1 Identificarea vulnerabilitatilor (sursei) si a conditiilor care ii influenteaza efectele (reducerea, cresterea)

In aceasta etapa a evaluarii sunt studiate urmatoarele aspecte:

- Trebuie determinat daca si in ce masura elementul relevant de sistem (sau elementul de resursa sau de infrastructura) afecteaza elementele de baza ale securitatii informatiilor (trebuie evaluat C/I/A individual al elementului relevant).
- Este necesar sa se examineze valorile C/I/A ale acestor elemente de sistem (sau elemente de resurse sau de infrastructura) in relatie intre ele.
- Trebuie evaluat care dintre amenintarile identificate anterior afecteaza elementele individuale.

3.2 Determinarea valorilor C/I/A ale sistemelor/elementelor sistemului, resurselor, elementelor de infrastructura

Valorile C/I/A sunt determinate pe baza principiilor generale de securitate pentru nivelurile de securitate, unde elementele individuale pot fi evaluate pe baza unui set uniform de criterii pentru activitatea/securitatea Bancii in ansamblu.

3.3 Listare detaliata si evaluarea vulnerabilitatilor

Pasii metodologici prin care vulnerabilitatile pot fi luate in considerare si evaluate sunt urmatorii:

- Revizuirea documentatiei disponibile,
- Colectarea de informatii de la utilizator(i) care opereaza/intretin sistemele/ elementele sistemului,
- Testarea practica a vulnerabilitatii sistemelor/elementelor sistemului.

3.4 Determinarea probabilitatii de exploatare cu succes a vulnerabilitatilor individuale

In aceasta faza a activitatilor de analiza se identifica sistemul (elementul) pentru care sunt relevante riscurile identificate in etapele anterioare. La identificarea amenintarilor (realizarea unui catalog de amenintari), probabilitatea de aparitie a fiecarei amenintari a fost identificata (cuantificata) in prealabil. Actualizarea catalogului se va realiza pe baza rezultatelor testelor de vulnerabilitate.

3.5 Stabilirea nivelului de risc rezidual

Riscul care ramane dupa implementarea noilor controale modificate reprezinta riscul rezidual. In general, nici un sistem IT nu este lipsit de riscuri si la toate masurile implementate nu se poate elimina riscul, dar nivelul de risc poate fi redus la nivel acceptabil.

Scaderea nivelului de risc reprezinta urmatoarea etapa a procesului de gestionare a riscurilor si presupune evaluarea optiunilor de reducere a riscurilor si punerea in aplicare a acestora, bazat pe prioritati.

Analiza in vederea scaderii riscului se face prin propunerea de masuri noi sau modificate in scopul de a reduce probabilitatea de manifestare a amenintarii care exploateaza vulnerabilitatile, si luand in considerare parametrii care definesc nivelul de risc.

Punerea in aplicare a unei masuri noi sau modificarea unui control existent poate reduce riscul de securitate prin:

- Eliminarea anumitor vulnerabilitati de sistem, in scopul de a reduce numarul de posibile amenintari/vulnerabilitati.
- Adaugare de masuri specifice, in scopul de a reduce sursele de amenintare.

4. Documentarea analizei de risc

Toate procesele de analiza a riscurilor efectuate si rezultatele acestora trebuie documentate. Analiza de risc este considerata finalizata numai dupa ce rezultatele acesteia au fost aduse la cunostinta conducerii superioare a Bancii.

4.1 Raportul de analiza a riscurilor

Raportul de evaluare a riscurilor va acoperi cel putin urmatoarele sectiuni/subiecte principale:

- scopul (pregatirea/revizuirea analizei de risc), domeniul de aplicare si metodologia analizei riscurilor,
- rezumat executiv, care prezinta pe scurt principalele constatari ale analizei riscurilor, principalele riscuri identificate si recomandarile pentru managementul acestora,
- amenintarile identificate/luate in considerare in timpul analizei de risc (catalog de amenintari),
- pregatirea unui catalog de risc care sa contina rezultatele analizei de risc intr-un rezumat de tabele,
- prezentarea detaliata, descriptiva a riscurilor identificate in analiza riscurilor inregistrate in Catalogul Riscurilor, dupa cum urmeaza:
  - Pe baza informatiilor colectate in timpul analizei riscurilor, riscurile generale valabile pentru organizatie in ansamblu, pe baza criticitatii lor si prezentate individual,
  - Pentru expunerile clasificate ca expunere la risc exceptional de ridicat/ridicat/mediu pentru fiecare element de sistem, defalcate pe niveluri de expunere la risc, un sistem (element) specific trebuie sa rezuma detaliile expunerii identificate (expunerile individuale si impacturile potentiale ale acestora),
  - Rezumatul riscurilor scazute/neglijabile pentru fiecare element de sistem, cu o scurta descriere a riscului pentru fiecare care ar putea fi demn de mentionat, dupa caz.
- un program de gestionare a riscurilor

4.2 Catalog de riscuri

Riscurile identificate in evaluarea riscurilor trebuie sa fie clasificate si prezentate intr-un format de tabel in functie de gravitatea/importanta acestora. Tabelul va include:

- identificatorul unic al riscului identificat
- o scurta descriere a riscului identificat
- numele elementului sistemului informatic sau unitatii organizationale implicate in risc

In baza analizei de risc efectuate si a catalogului de riscuri rezultat, se va elabora un raport care va contine pasii de atenuare a riscurilor cel putin pentru riscurile clasificate ca expunere la risc exceptional de inalta/inalta/medie.

Acesta va putea fi folosit ca baza pentru implementarea unui program de gestionare a riscurilor, care trebuie monitorizat si revizuit minim anual, de catre echipa de Management al Riscului din cadrul bancii.

Experienta similara:

Client	**Descriere proiect**	**Perioada**
Fan Courier	Servicii de consultanta pentru elaborarea unei analize de tip BIA pentru Fan Curier	22.08.2022 – 30.12.2022
Idea Bank	Servicii de analiza interna si elaborare a unei analize de impact asupra afacerii (BIA)	30.06.2020 – 15.08.2020
OTP Bank	Servicii de auditare EBA/GL/2019/04	18.04.2023 - 15.09.2023
PAID Romania	Activitati de Management al riscului in domeniul Tehnologiei Informatiei si Comunicarii (TIC)	01.11.2024 - prezent
Idea Bank	Servicii de asigurare a conformitatii si securitatii sistemelor informationale in conformitate cu cerintele Ghidului Autoritatii Bancare Europene privind administrarea riscurilor TIC si de securitate (EBA/GL/2019/04) si de auditare cu privire la riscurile TIC	20.07.2023 – 15.09.2023

B. Servicii de audit a securității soluției de plăți instant

Auditul se va desfasura conform standardelor internaţionale de audit în domeniul sistemelor informaţionale, va exprima opinia de audit privind suficienţa şi eficienţa măsurilor de securitate implementate aferente utilizării soluției de plăți instant, gestiunea atacurilor cibernetice și conformarea cu standardele internaționale și cele mai bune practici în domeniu.

Raportul de audit va conţine referinţe la probele de audit utilizate şi concluziile pentru următoarele obiective de audit:

- Cadrul normativ intern aferent soluției de plăți instant;
- Securitatea datelor;
- Identificarea și autentificarea utilizatorilor;
- Performanța și scalabilitatea soluției;
- Confidentialitatea, integritatea, disponibilitatea și non-repudierea tranzacțiilor;
- Managementul identităților și segregarea responsabilităților;
- Mijloace de control pentru autorizarea la nivelul sistemelor, bazelor de date și aplicației;
- Fraude interne și externe;
- Jurnale de audit;
- Confidențialitatea informației în procesul transportului de date;
- Riscul de securitate aferent terților părți;
- Securitatea fizică;
- Gestionarea incidentelor;
- Gestiunea vulnerabilităților;

- Continuitatea funționării sistemului.

În cadrul misiunii de audit se va evalua eficiența controalelor de securitate implementate prin teste specifice de securitate testînd eficacitatea măsurilor de securitate control implementate pentru reducerea riscurilor identificate ca urmare a analizei de riscuri efectuate prin simularea unor atacuri specifice riscurilor identificate.

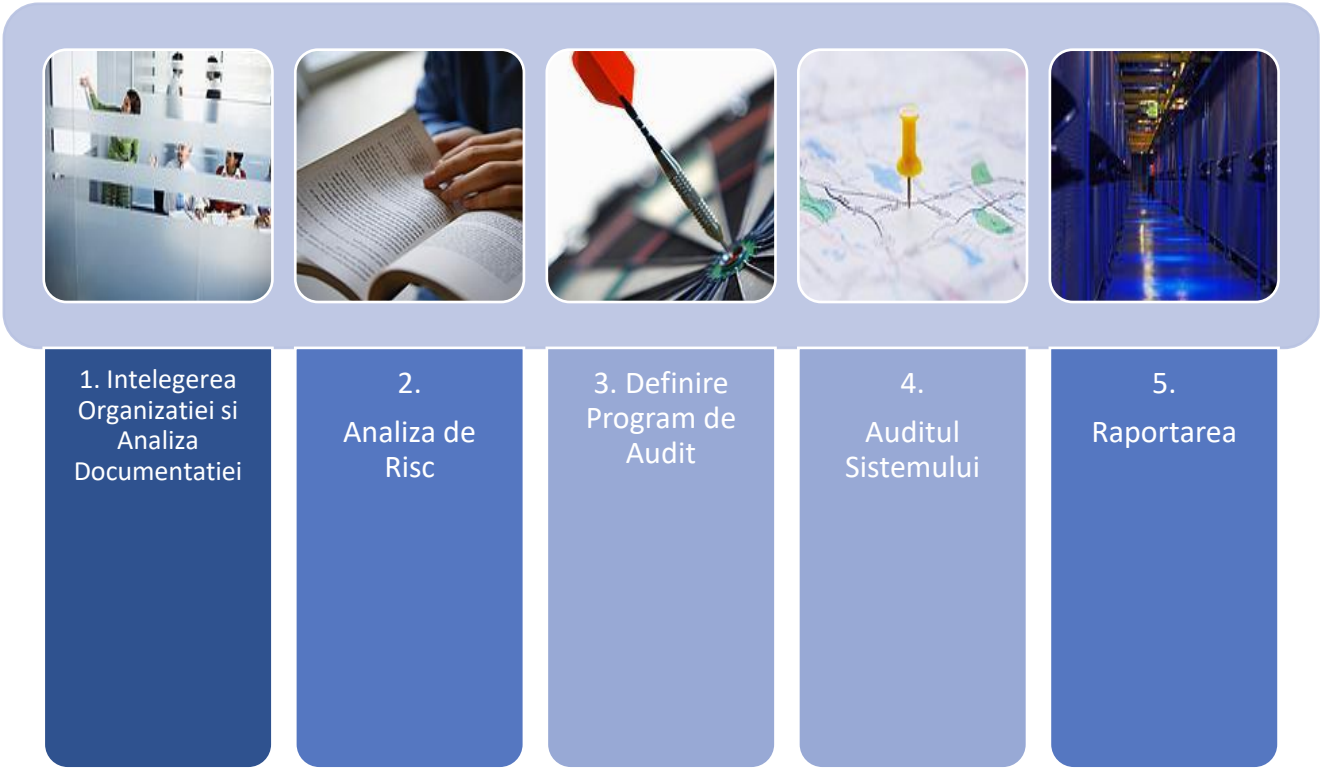
Metodologia serviciilor de audit a securității soluției de plăți instant

Scopul serviciului este de a determina riscurile de securitate asociate solutiei de plati instant. In acest sens, FORT va realiza un audit independent al planului de securitate si a solutiei informatice prin intermediul caruia este oferit serviciul. In urma activitatilor de audit, FORT va emite o opinie de audit si o declaratie privind independenta auditorului, insotite de raportul de audit. Auditul va urmari existenta unor masuri concrete in ceea ce priveste:

- confidentialitatea si integritatea comunicatiilor;
- confidentialitatea si nonrepudierea tranzactiilor;
- confidentialitatea si integritatea datelor;
- autenticitatea partilor care participa la tranzactii;
- protectia datelor cu caracter personal;
- pastrarea secretului bancar;
- trasabilitatea tranzactiilor;
- continuitatea serviciilor oferite clientilor;
- impiedicarea, detectarea si monitorizarea accesului neautorizat in sistem;
- restaurarea informatiilor gestionate de sistem in cazul unor calamitati naturale, evenimente imprevizibile;
- gestionarea si administrarea sistemului informatic;
- orice alte activitati sau masuri tehnice intreprinse pentru exploatarea in siguranta a sistemului.

1. Etapizare Audit

In vederea construirii unei opinii obiective, echipa de audit va realiza urmatoarele activitati



I. Intelegerea organizatiei si analiza documentatiei

Intelegerea organizatiei presupune culegerea de informatii relevante pentru etapele urmatoare. Aceste informatii includ: detalii despre organizarea interna, detalii despre organizarea IT, despre tehnologii si sistemele

folosite, modul de functionare al Sistemelor de Plati Instant (SPI), cat si restul documentelor mentionate ca prerechizite in cadrul etapelor ulterioare. In mod normal, echipa de consultanta va programa interviuri cu persoanele responsabile desemnate de catre banca, sau, dupa caz, va folosi chestionare pentru fiecare sectiune in parte. Tot in aceasta etapa se va realiza o lista cu rolurile si responsabilitatile personalului bancii in administrarea si operarea SPI.

In continuare:

- Se va evalua documentatia (Plan securitate, proceduri)
- Se vor formula recomandari pentru imbunatatirea documentatiei,
- Banca va realiza implementarea celor mai importante recomandari,
- Se va verifica includerea recomandarilor in Planul de securitate si documentele aferente.

II. Analiza de risc si definirea programului de audit

Analiza riscurilor nu este numai o cerinta legala, dar si o baza pentru crearea si executia programului de audit. Astfel, verificarile intreprinse vor avea in vedere expunerea pe care o au sistemul si informatiile gestionate la riscuri privind securitatea informatiilor.

In vederea realizarii acestei analize de risc, se vor realiza urmatoarele:

a. Identificarea elementelor analizate: sisteme, aplicatii, procese, oameni
b. Identificarea vulnerabilitatilor si a amenintarilor
c. Cuantificarea si masurarea scenariilor de risc
d. Identificarea controalelor aplicabile
e. Stabilirea registrului de riscuri si identificarea riscurilor reziduale sau a scenariilor necotrolate

In baza riscurilor evidentiate in faza de evaluare a riscurilor, auditorul va defini programul de audit care se va folosi in fazele ulterioare. Programul de audit are ca scop definirea de obiective de control si de verificari care se vor intrebuinta in verificarile la fata locului. Tot programul de audit specifica si criteriile de masurare penru stabilirea conformitatii cu cerintele legale prinvind masurile minime de securitate adoptate.

III. Auditul sistemelor

In cadrul acestei faze, echipa de auditori va intreprinde evaluarile si testele prevazute in programul de audit, cu scopul de a verifica atingerea obiectivelor de control stabilite.

Acesta cuprinde 7 componente principale:

- Revizuirea controalelor tehnice implementate la nivelul aplicatiilor de Internet si Home Banking
- Revizuirea controalelor tehnice implementate la nivelul serverelor ce sustin sistemele si Interfetele acestora catre sistemul inima
- Revizuirea controalelor tehnice implementate la nivelul infrastructurii de retea
- Revizuirea controalelor de acces fizic
- Revizuirea procedurilor operationale ale sistemelor
- Revizuirea procedurilor de mentenanta si recuperare in caz de dezastru
- Revizuirea controalelor tehnice implementate la nivelul statiilor de lucru
- Raportare

Aspecte generale:

- Se vor evalua configuratiile echipamentelor ce asigura securitatea retelei (router, firewall, IDS, etc.) din punctul de vedere al securitatii, pe baza recomandarilor producatorilor si a practicilor din industrie. Configuratiile vor fi puse la dispozitie de administratorii sistemelor respective.
- Se vor evalua configuratiile serverelor critice din punctul de vedere al securitatii, pe baza recomandarilor producatorilor si a practicilor din industrie. Accesul la consola serverelor se va face cu suportul administratorilor sistemelor respective.
- Se vor purta discutii cu personalul cheie, implicat in adminsitrarea si operarea sistemului, cu scopul de a determina conformitatea proceselor sau de a stabili puncte de vulnerabilitate in procesele descrise.
- Se vor analiza documente si inregistrari care sustin existenta proceselor descrise in documentatie.

1. Revizuirea controalelor tehnice implementate la nivelul aplicatiilor de Internet si Mobile Banking

Verificarile vor urmari identificarea controalelor de securitate implementate la acest nivel si conformitatea aplicatiei cu bunele practici. Vor fi analizate procesele de autentificare, autorizare si jurnalizare, modul de stocare al datelor, comunicatia cu SGBD-urile, protectia datelor sensibile sau de autentificare, metodele de alertare, canalele de comunicatie cu utilizatorii serviciului, mecanismele de transmitere si validare a datelor de catre aplicatie, etc.

2. Revizuirea controalelor tehnice implementate la nivelul serverelor ce sustin sistemele si Interfetele acestora catre sistemul inima

Sistemele inspectate vor cuprinde in functie de sistemul auditat:

- Servere Web
- Servere de Baze de Date
- Servere de nume
- Servere de domeniu
- Mediul de test
- Servere de interfatare Core Banking sau cu alte subsisteme bancare

La nivelul serverelor vor fi analizate:

- Politica de management centralizat
- Politica de administrare la distanta
- Politica de parole
- Politica de update si de instalare de aplicatii software
- Politica de Change management
- Politica de jurnalizare si audit
- Politica de monitorizare a componentelor hardware si software
- Controalele punctuale aplicate in cazul management-ului local
- Permisiunile de acces administrativ
- Configuratia firewall-ului local
- Serviciile active
- Porturile active
- Aspectele referitoare la virtualizare
- Controalele impotriva virusilor / troienilor

3. Revizuirea controalelor tehnice implementate la nivelul infrastructurii de retea

Controalele vizeaza inspectarea echipamentelor de tip:

- Routing & Switching
- Firewall
- IDS / IPS
- Acces la distanta (VPN)

La nivelul infrastructurii de retea vor fi analizate:

- Controalele de securitate implementate in LAN
- Controalele de securitate pentru WAN
- Politica de agregare si segmentare a traficului
- Politica de inspectare a traficului
- Fluxurile de informatie dinspre si catre serverele din sistemul auditat
- Permisiunile de acces la distanta
- Controalele de securitate la nivelul dispozitivului de retea
- Controalele de securitate impotriva atacurilor de tip DoS
- Politica de redundanta la nivelul retelei
- Politica de monitorizare la nivelul retelei
- Logurile si alertele generate de echipamentele dedicate
- Politica de update
- Politica de Change management

4. Revizuirea controalelor de securitate fizica

Controalele de securitate vor fi revizuite pentru centrul de date unde ruleaza sistemul.

Acestea vor cuprinde:

- Metodele de acces
- Protectia impotriva hazardelor si a dezastrelor

5. Revizuirea procedurilor operationale ale sistemului
6. Revizuirea procedurilor de mentenanta si recuperare in caz de dezastru
   - Politica de backup
   - Politica de restaurare
7. Politica de recuperare in caz de dezastru

Revizuirea controalelor tehnice implementate la nivelul statiilor de lucru

Impreuna cu reprezentantii bancii vor fi alese statii de lucru relevante pentru sistemul auditat, pentru care vor fi inspectate urmatoarele:

- Politica de management centralizat
- Politica de firewall
- Politica de Patch Management
- Politica de Change Management
- Politica de acces
- Politica de parole
- Politica de audit
- Politica de monitorizare si alertare (hardware si software)
- Permisiunile locale
- Serviciile active

IV. Raportarea

Activitatile de audit se vor incheia prin livrarea raportului de audit.

a. Raportul de audit. Acest livrabil va documenta operatiunile si testele intreprinse.
   i. Vor fi documentate neconformitatile, observatiile si recomandarile pentru imbunatatire
   ii. Neconformitatile reprezinta neconcordante intre sistemul existent cu documentatia pregatita de banca (Planul de securitate) sau aspecte care, in mod evident, incalca conditiile minime de securitate
   iii. Observatiile reprezinta aspecte care duc la periclitarea starii de securitate a sistemului si care pot conduce, in anumite conditii, la nerespectarea conditiilor minime de securitate
   iv. Recomandarile privind imbunatatirile nu semnaleaza probleme de securitate, insa sunt menite sa aduca imbunatatiri sistemului de management al securitatii informatiilor.

b. Declaratia privind independenta auditorului – certifica aspectele care privesc independenta auditorului si confirma inexistenta aspectelor care ar putea sa afecteze obiectivitatea auditului.

V. Livrabile

In urma activitatilor de mai sus, vor fi livrate urmatoarele rapoarte, asa cum au fost detaliate anterior:

1. Declaratie de independenta a auditorilor fata de sistemul informatic auditat. Acest document se emite in limba romana, intr-un exemplar original.
2. Raportul de audit continand metodologia utilizata, concluzii, constatari si recomandari. Raportul de audit este emis in atentia si pentru uzul bancii. Acest document include textul primelor doua livrabile, se emite in limba romana, livrandu-se un exemplar electronic si unul tiparit
3. Raportul de analiza asupra controalelor de securitate continand observatiile echipei de audit asupra controalelor implementate si a celor aplicabile, recomandari, concluzii.

C. Testarea de securitate

Testele ce urmează să se desfășoare se vor efectua conform celor mai bune practici în domeniu (OWASP, NIST, PTES, OSSTMM, CREST, ISO, CIS, MITRE ATT&CK Framework) și vor implica:

- teste efectuate din rețeaua externă a BNM;
- teste efectuate din rețeaua internă a BNM;
- evaluări ale vulnerabilităților;
- teste de reziliență operațională:
- simulări privind volumul de tranzacții;

- simulări ale căderilor de sistem și recuperarea acestora;
- simularea atacurilor de tip DoS/DDoS.

Testele se vor derula în trei etape distincte, și anume:

1. Pre-evaluare (Pre-assesment)
2. Evaluare (Assesment)
3. Post-evaluare (Post-assesment)

Etapa de Pre-evaluare (Pre-assesment) – reprezintă faza premergătoare evaluării și este importantă pentru determinarea specificațiilor precise și a regulilor de desfășurare a evaluării. În această etapă se vor stabili și elabora Planul de testare, Planul de acțiuni (SOW – State of Work), precum și, scenariile de atac, și se vor obține autorizațiile necesare desfășurării testelor. Această etapă se va desfășura pe parcursul numărului de zile lucrătoare detaliat în cadrul planului de proiect și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor detalia:

- activitățile întreprinse;
- resursele incluse în activitatea de testare;
- termenul propus de realizare;
- persoane responsabile din partea Beneficiarului și a Prestatorului.

Etapa de Evaluare (Assesment) – reprezintă etapa de derulare propriu-zisă a testelor de securitate.

Această etapă a testării include evaluarea conectivității între sistemele utilizate pentru test și sistemele testate, culegerea informațiilor despre sistemele testate, descoperirea sistemelor și serviciilor active, precum și, scanarea sistemelor pentru descoperirea vulnerabilităților. Utilizînd informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac și se vor implementa acțiunile definite în aceste structuri. Testele efectuate vor fi făcute urmărind scenarii de atat din externul rețelei BNM și din rețeaua internă a BNM. De asemenea, scenariile vor include atacuri la nivelul tuturor utilizatorilor ce au acces la soluția de plăți instant. De asemenea, va avea loc simularea de atacuri cibernetice asupra sistemului folosind tehnici avansate de compromitere a securității informației, pentru a identifica vulnerabilități și potențiale breșe de securitate, evaluarea configurărilor de securitate, a politicilor de acces și a altor măsuri de protecție existente. În același context se va face documentarea vulnerabilităților detectate, gradul de severitate al acestora și riscurile asociate. Nu în ultimul rînd va avea loc testarea masurilor de control recomandate și reconfigurărilor propuse în cadrul etapei de pre-evaluare. Etapa de Post-evaluare (Post-assesment) – această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de analiză, a rezultatelor testelor efectuate în care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact. În această etapă Prestatorul va acorda suport Beneficiarului pentru înțelegerea deplină a problemelor identificate și recomandarea măsurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite. Totodată Prestatorul var-testarea anumitor componente, pentru a verifica aplicarea corectă a măsurilor de remediere recomandate.

Testele ce se vor efectua sunt:

- teste efectuate din rețeaua externă a BNM;
- teste efectuate din rețeaua internă a BNM;
- evaluări ale vulnerabilităților;
- teste de reziliență operațională:
- simulări privind volumul de tranzacții;
- simulări ale căderilor de sistem și recuperarea acestora;
- simularea atacurilor de tip DoS/DDoS.

Metodologia utilizata pentru fiecare in parte, precum si activitatile ce vor fi realizate, este descrisa mai jos.

Metodologii aplicabile

1.1 Metodologia de evaluare a securității

Conform standardelor de evaluare a sistemelor informatice, vom face cunoscute următoarele:

1.1.1 Autoritate

Evaluatorii vor avea autoritatea de a-și dezvolta activitățile. În timpul proiectului, aceștia vor avea acces la anumite informații, resurse și spații fizice care în mod normal nu sunt disponibile. Persoanele îndreptățite să permită accesul la aceste informații sau resurse vor fi informate cu privire la legitimitatea abordării noastre. De asemenea, oamenii din companie, pentru a fi intervievați sau pentru a facilita accesul la informații vor trebui să acționeze cu profesionalism și responsabilitate, oferind toate informațiile pe care le avem despre subiect fără modificări sau nuanțe. Este interesul beneficiarului ca opiniile exprimate să se bazeze pe informații reale și actuale.

1.1.2 Confidențialitate

Informațiile la care vor avea acces evaluatorii sunt confidențiale. Se angajează să mențină confidențialitatea și confidențialitatea informațiilor obținute în timpul proiectului; Aceste informații nu pot fi utilizate pentru persoane sau terți, cu excepția cazurilor prevăzute de lege.

Concluziile și informațiile pe care se bazează vor fi arhivate de evaluatori pentru a susține validitatea avizului pe care îl furnizează în cazurile cerute de lege sau când aceștia la rândul lor vor fi auditați de autoritățile competente...

1.1.3 Independență

Inainte de semnarea contractului, vom discuta despre managementul companiei cu evaluatorul beneficiar probleme de independenta.

Evaluatorii și experții care participă la evaluare trebuie să fie poziționați independent de subiect și de organizația evaluată, astfel încât:

- Nu există niciun conflict de interese între rolul evaluatorilor și alte roluri, cum ar fi consultantul; Astfel, evaluatorii selectați nu au făcut parte dintr-o echipă de proiect pentru activități de consultanță și implementare care afectează sistemul inspectat. De asemenea, fiind o evaluare externă și independentă, evaluatorul nu poate fi angajat de organizația sau organizațiile client din același grup.
- Evaluatorul nu are interese financiare comune cu organizația evaluată (altele decât valoarea contractului); Astfel, evaluatorul nu este un acționar sau organizație parteneră de la care și-a îndeplinit misiunea și nu poate avea beneficii financiare directe și imediate după formularea unei recomandări

În orice moment, în cazul în care independența evaluatorului poate fi pusă la îndoială, va fi informat cu privire la toate părțile (furnizor și client) motivele existente; acesta din urmă va fi revizuit pentru activitățile proiectului vor fi încheiate; Evaluarea va continua cu aceiași evaluatori după clarificarea aspectelor de independență.

1.1.4 Cerințe specifice pentru evaluator

Organizația trebuie să informeze persoanele implicate despre proiect și să se asigure că aceste persoane sunt disponibile pentru această acțiune. Cu excepția activităților dublu-orb cu cutie neagră.

De asemenea, este de dorit ca evaluatorii să primească toate documentele (plan de securitate, sisteme de descriere etc.) în format electronic.

Reprezentanții beneficiarului nu vor încerca să influențeze rezultatul proiectului prin intimidarea membrilor echipei de evaluare prin furnizarea de informații false sau prin condiționarea acceptării plății pentru livrabile sau rezultatul proiectului.

1.1.5 Criterii de măsurare a calității și acceptării

Rezultatele de mai sus reprezintă constatările sau opiniile evaluării, deci este imposibil să se definească criterii de măsurare a calității. Înainte de emiterea raportului, concluziile și dovezile pe care se bazează vor fi discutate cu conducerea companiei pentru a asigura conformitatea cu realitatea concluziilor noastre.

Receptia livrabilelor va fi considerata acceptare. În caz de îndoială, evaluatorii vor efectua opinii bazate pe dovezi/dovezi obiective dezvăluite în timpul proiectului.

1.1.6 Codul de etică

Evaluatorii noștri s-au alăturat următorului cod de etică:

1. Sprijină și încurajează respectarea standardelor, procedurilor și controalelor aplicabile sistemelor informatice
2. Să demonstreze obiectivitate și profesionalism în îndeplinirea activității de evaluare
3. Păstrează standardele înalte de conduită și comportament și nu se vor angaja în activități care i-ar putea discredita, asupra organizațiilor pe care le reprezintă sau asupra beneficiarilor
4. Păstrarea confidențialității și confidențialității informațiilor obținute în timpul proiectului; Aceste informații nu pot fi utilizate pentru scop personal sau pentru terți, cu excepția cazului în care este cerut de lege.
5. Menține un nivel ridicat de expertiză în domeniile lor de specializare.
6. Informați toate părțile îndreptățite să primească aceste informații despre rezultatul acțiunilor lor.

1.2 Metodologia de evaluare a vulnerabilității

Prin acest serviciu, echipa de evaluare își propune să identifice vulnerabilitățile prezente în sistemul informatic într-o abordare practică și eficientă. Spre deosebire de un audit general al sistemelor informatice, care vizează obținerea unei asigurări rezonabile a managementului securității, evaluarea vulnerabilității IT include verificarea și analiza reală a sistemelor și serviciilor IT accesibile din poziția atacatorului.

Beneficii

Verificările urmează orice etapă de atac informatic, prin care potențialul atacator real ar încerca să compromită securitatea unui sistem țintă (poziția "cutie neagră"). Având în vedere că niciun sistem nu este complet sigur, factorul determinant în evaluarea probabilității unui atac de succes este determinat în mare măsură de elementul timp.

Din perspectiva unui atacator profesionist, valoarea atacului este coeficientul dintre rezultatul obținut și timpul necesar executării cu succes.

Serviciul oferit reprezinta analiza suprafetei expuse atacului unui sistem informatic, precum si identificarea vulnerabilitatilor care pot fi exploatate de catre un atacator pentru a compromite cu succes sistemul tinta.

Activităţi

Activitățile vizează toate acțiunile desfășurate într-un scenariu real de verificare a suprafeței de atac, împreună cu opțiunile de remediere cu ale lor.

- Descoperire - Identificarea sistemelor expuse
- Enumerare - Identificarea serviciilor disponibile și particularitățile acestora (versiuni, module, sisteme de operare)
- Analiză - Verificarea prezenței unui set larg de vulnerabilități pe serviciul țintă
- Prezentare și remediere - Ilustrarea suprafeței de atac care cuprinde riscul vulnerabilităților tehnice urmărite, cu opțiuni de remediere a acestora

Raport

- Rezumat - Oferă concluzii cu privire la nivelul de risc asociat cu suprafața de atac a sistemului evaluat
- Vulnerabilități identificate - Prezentarea fiecărei vulnerabilități cu exploatarea cu succes a acestui impact și opțiuni de remediere
- Lecturi suplimentare despre atacuri - Referințe la resurse externe privind vulnerabilități specifice
- Glosar - Definiții ale termenilor tehnici utilizați în livrabile.

1.3 Metodologia de testare a penetrării

Testarea de penetrare efectuează o analiză complexă a auditului de securitate a sistemului informatic, testând eficacitatea măsurilor de securitate implementate prin executarea atacurilor reale. Activitățile se bazează pe practica "hackingului etic". Acestea sunt metode utilizate atacatori reali globali sunt aplicate și personalizate sistemului țintă într-un mediu controlat. Testele pot fi efectuate atât într-o poziție "cutie neagră" - echipa de audit se află într-o poziție de organizație externă de atac, fără nicio informație despre sistem, cât și din postări "casetă gri/albă" - folosind informații care au acces regulat la un angajat (utilizator business) și un angajat IT (angajat IT). Spre deosebire de scanările de vulnerabilitate, penetrarea testelor depășește absența patch-urilor de porturi deschise și riscurile potențiale teoretice, ajungând să treacă de bariere de securitate eficiente prin încercarea de a exploata vulnerabilitățile sistemului, inclusiv chiar eroarea umană prin procedurile de "inginerie socială".

Deși activitățile se pot desfășura direct în mediul de producție, atacurile sunt atent controlate, iar cele care pot afecta funcționalitatea sistemului sunt lansate după scenarii bine dezvoltate și convenite în prealabil cu clienții noștri.

Scopul urmărit în cadrul activităților de evaluare este de a identifica și documenta încălcările de sistem privind:

- Autentificare - mecanisme prin care utilizatorii sunt identificați, autentificați și autorizați să utilizeze funcțiile sistemului
- Validarea tranzacțiilor - mecanisme prin care tranzacțiile introduse de utilizator sunt acceptate și procesate de sistem
- Confidențialitatea tranzacțiilor - măsuri implementate pentru a împiedica accesul la detaliile tranzacțiilor efectuate de persoane neautorizate
- Confidențialitatea datelor - măsuri implementate pentru a împiedica accesul la datele clienților (nume, adresă, informații de contact, nume de utilizator etc.) de către persoane neautorizate
- Disponibilitatea serviciului - aspecte legate de furnizarea neîntreruptă a sistemului

Testele vor lua în considerare vulnerabilitățile care au apărut în timpul ciclului de viață al aplicației: planificare, proiectare, dezvoltare, implementare, operare, întreținere și chiar eliminare.

Identificarea oricăror încălcări, inclusiv documentația și problemele de asistență identificate prin dovezi obiective, care se încadrează în categoriile de mai sus reprezintă succesul afacerii noastre

Rezultat

Testele de penetrare reprezintă verificarea supremă a sistemului de securitate. Acesta este cel mai dur și elocvent test de identificare a vulnerabilităților care pot fi exploatate în practică de un hacker care este motivat să compromită securitatea unei organizații.

Beneficii:

- Obținerea unei opinii convingătoare, obiective și corecte despre vulnerabilitățile care ar putea compromite organizația de securitate (vulnerabilitățile sunt inerente; asigurați-vă că sunteți primul care le descoperă)
- Obținerea unui grad ridicat de conștientizare a securității în rândul angajaților și personalului IT. A fi atacat de o echipă de testeri de penetrare este cel mai bun mod de a-ți instrui oamenii cu privire la securitatea IT, făcându-i să înțeleagă ce s-ar fi întâmplat în viața reală.
- Transferul de cunoștințe cu privire la remedii, arătând cum sunt făcute, cum să se remedieze și ce ar trebui făcut pentru a preveni viitorul.
- Capacitățile de evaluare, implementare și optimizare pentru răspunsul la incidente din cadrul organizației. Cum am dus organizația ta să detecteze atacul? Dar să reacționeze? A fost un succes, sunt lecții de învățat?
- Raportul testelor este o intrare relevantă pentru managementul riscului IT / managementul riscului operațional

Testele de penetrare efectuate sunt esențiale pentru a avea o imagine reală a stării sistemului de securitate. Considerăm că orice sistem care gestionează date critice pentru procesele de business trebuie supus periodic unor astfel de teste, așa cum impun cele mai exigente standarde din domeniu (cum ar fi PCI DSS).

Raport

- Rezumat - Oferă concluzii cu privire la nivelul de risc asociat cu suprafața de atac a sistemului evaluat
- Vulnerabilități identificate - Prezentarea fiecărei vulnerabilități cu exploatarea cu succes, clasificarea impactului acesteia și opțiunile de remediere
- Lecturi suplimentare despre atacuri - Referințe la resurse externe privind vulnerabilități specifice
- Glosar - Definiții ale termenilor tehnici utilizați în livrabile.

Remediation roadmap va acoperi:

1. Matricea de vulnerabilități clasificate după principiile clientului / recomandarea FORT
2. Evaluarea riscurilor reziduale identificate
3. Opțiuni de remediere prioritare (tehnice/de proces)
4. Plan tactic de remediere, inclusiv estimări de efort/timp/buget, dacă este necesar
5. Analiza SWOT a securității informațiilor

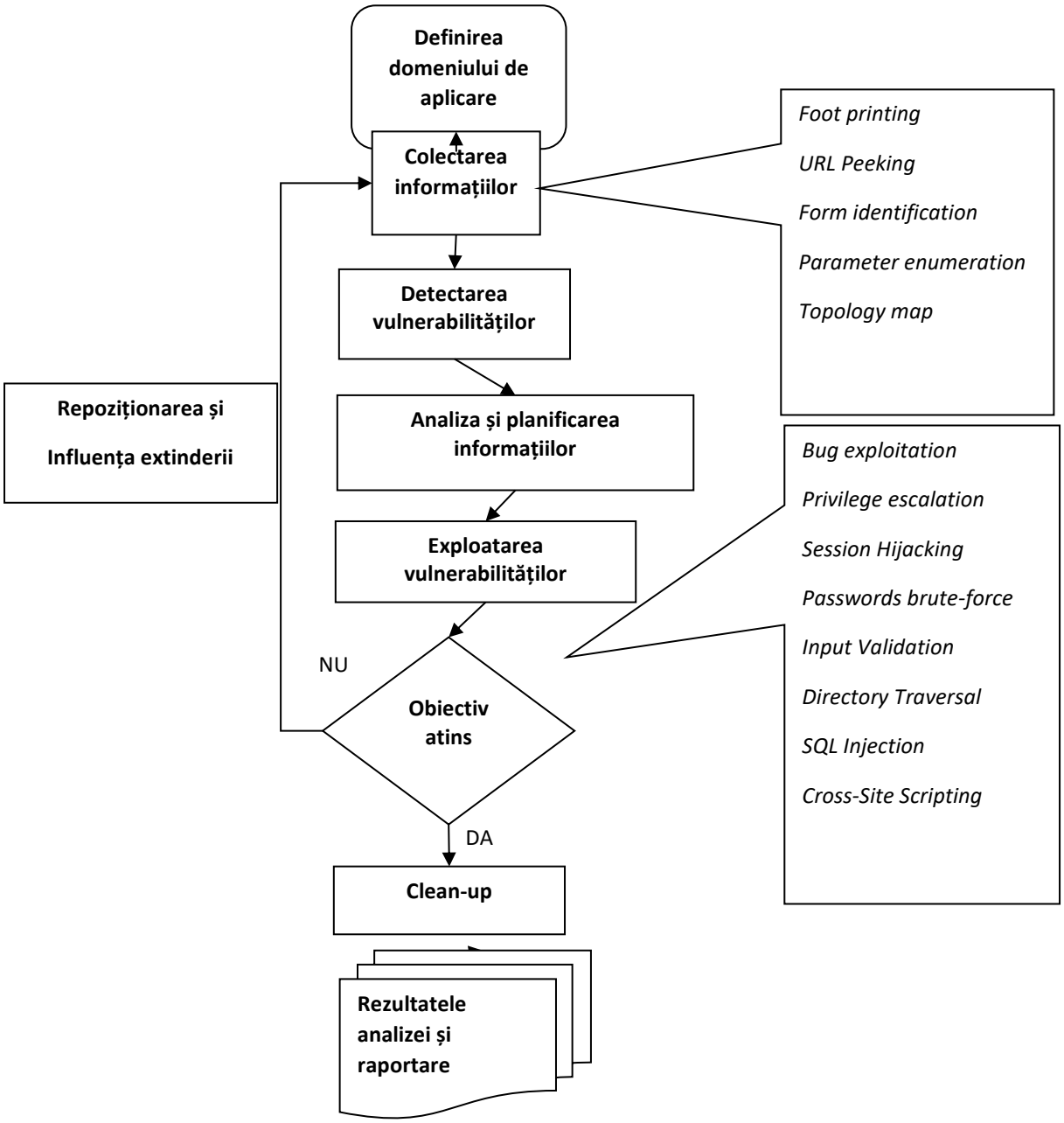
Acreditari ale echipei FORT:

- Offensive Security Certified Professional – OSCP, Offensive Security
- Certified Information Systems Security Professional – CISSP, ISC2
- Systems Security Certified Professional - SSCP, ISC2
- ISO 27001 Lead Auditor – BSI
- ISO 9001:2000 Specialist
- EC-Council Certified Security Analyst (ECSA)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA) – ISACA
- Certified Information Systems Manager (CISM) – ISACA
- Certified in the Governance of Enterprise Information Technology (CGEIT) – ISACA
- Certified in Risk and Information Systems Control (CRISC) - ISACA
- Licensed Penetration Tester (LPT)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Incident Handler (GCIH)
- GIAC Exploit Researcher and Advanced Penetration
- GIAC Penetration Tester (GPEN)
- Offensive Security Wireless Professional
- ITIL FOUNDATION
- Programming Mobile Applications for Android Handheld

- ISTQB (R) Certified Tester, Foundation Level
- Microsoft Certified Technical Specialist (MCTS)
- Microsoft Certified Professional Developer (MCDP)
- IT Infrastructure Library v3 Foundation (ITILv3)
- ITIL Expert;
- OCMJD (Oracle Certified Master Java Developer);
- Microsoft Certified Professional (MCP)
- ISO 9001:2000 Internal Quality System Auditor
- ISO 27001 Lead Auditor
- Fortinet Certified Network Security Professional 2015
- Fortinet Certified Network Security Administrator 2014
- Managing Office 365 Identities and Requirements 2014
- Server Virtualization with Windows Server Hyper-V
- Windows 7, Enterprise Desktop Administrator
- Administering Office 365 for Small Business
- Windows Server 2008 R2, Server Virtualization
- Windows Server 2008 Active Directory, Configuring
- Windows Server 2008 Network Infrastructure, Configuring
- Windows Server 2008, Server Administrator
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Security Professional (CCNP)
- Cisco Certified Design Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Design Associate (CCDA)
- Cisco Certified Academy Instructor (CCAI)
- RedHat Certified Engineer (RHCE)
- Fortinet Certified Network Security Associate (FCNSA)
- Fortinet Certified Network Security Professional (FCNSP)
- INFOSEC 4011 Recognition (NSA & CNSS)

- Project Management Professional (PMP)
- Certified Associated Project Manager (CAPM)

Metodologia generală utilizată de serviciile FORT în evaluarea și testarea sistemelor de securitate este sintetizată în următoarea diagramă:



În acest proces, FORT desfășoară următoarele activități:

Definirea domeniului de aplicare a evaluării

- La inceputul proiectului, impreuna cu beneficiarul se va defini acoperirea ariei de evaluare
- Stabilirea modului de simulare a atacurilor
- Stabilirea nivelului de agresivitate al atacului: cât de departe va merge cu încercările de exploatare a unei vulnerabilități

- Colectarea informațiilor disponibile public despre sistemul informatic al companiei
  - Informațiile conținute pe site-ul companiei, informațiile conținute în înregistrările Whois, DNS, RNC
  - Informații despre sistemul informatic al companiei care pot fi obținute din alte surse.
- Detectarea vulnerabilităților
  - Folosind software și metode specializate, cunoscute în industrie pe baza informațiilor colectate din fazele anterioare, se vor identifica sistemele care sunt active în rețea, rulând servicii;
  - Identificați sistemele de operare și versiunile serviciului activ.
- Analiza rezultatelor și raportarea
  - Vor fi analizate informațiile rezultate din detectarea fazei vulnerabilităților
  - Existența vulnerabilităților majore va fi confirmată prin analiza sistemelor individuale implicate
- Identificarea și analiza mijloacelor de îmbunătățire, formularea recomandărilor
  - Pe baza constatărilor din paragrafele anterioare va formula recomandări concrete pentru remedierea oricăror vulnerabilități. Acesta va include trimitere directă la documentația producătorului sau prin alte surse disponibile pentru remedierea vulnerabilității
- Operațiuni documentare efectuate și rezultate
  - Metodologia utilizată, constatările, vulnerabilitățile identificate și recomandările vor fi documentate

Metodologia utilizată se bazează pe metodologia de testare a securității Open Source – OSSTM versiunea 3.0.

Security Services Statement of Work

External Infrastructure Pentest

Attack posture: blackbox double-blind

Activitati:

- Reconnaissance (IP, DNS, Social Media, etc.)
- Testing firewall (firewalking, fragmentation, etc.)
- Discovery of the services – TCP/IP scanning, OS fingerprinting, banner grabbing, etc.
- Credentials hacking – enumeration, spraying, brute force, dictionary, mixed, etc.
- Google Hacking
- Specific vulnerability analysis systems in-scope
- Identifying vulnerabilities in the design

- Identifying vulnerabilities in the implementation / configuration
- Identifying vulnerabilities in the design and implementation of security policies
- Blackbox evaluation of design and implementation of VPN and remote access policies
- Exploitation of the specific vulnerabilities of externally exposed services
- Cracking of credentials using dictionary / brute-force / hybrid / spraying attacks
- MITM attempts, sniffing, spoofing
- Identification of backdoors, unsafe remote access gates
- DoS/DDoS amplification/logic bomb attacks

Target of evaluation (service coverage area):

- Operating systems /Firmware
- Turned on services and associated modules loaded
- Active protocols (client-server, administrative, switching, routing, etc.)
- Configuration server / network equipment
- Configuration of the services

Web Application Penetration Testing (daca este cazul)

Attack posture: blackbox internal & external, credentialed

Activități:

- Input Validation Attacks
- Access Control Attacks
- Authentication & Session (bypass, session hijacking, session fixation)
- Cross Site Scripting (XSS)
- Error Treatment / Sensitive Data Leakage
- Credential cracking (password spraying, brute-force, dictionary attacks)
- Injection of arbitrary code - basic
    - SQL Injection
    - XPATH Injection
    - LDAP Injection
- Insecure Object References resulting in LFI/RFI (Local/Remote File Inclusion)
- RCE (Remote Command Execution)
- Application/infrastructure configuration errors
- Horizontal escalation of privileges (eg, accessing data of other patients or doctor)
- Vertical escalation of privileges (eg the access security context of a user in another profile, access account a patient at the doctor)
- Public vulnerabilities type Common Gateway Interface (CGI)
- Obtaining information from the public domain
- Inter-Domain Attacks (CSRF)
- Application-specific vulnerabilities (AJAX, Flash, ActiveX)
- Scanning Applications from SOW using automated tools and manual tests
- Enumeration techniques
- Simple Business Logic attacks
- Simple cryptographic / encryption attacks
- Unvalidated redirects and forwards
- Gaining unauthorized access by exploiting vulnerabilities
- The consolidation of access
- Removal of traces in the attack and other proofs of the access
- Web Services-specific tests
    - WS Information Gathering
    - Testing WSDL
- Replay Testing

- SPA (Single-Page Application) specific security testing

Vulnerability Assessment – external

Activitati:

- Authentication (bypass, session hijacking, session fixation)
- Cross Site Scripting (XSS)
- Buffer overflow
- Treatment of errors
- Injection of arbitrary code
- SQL Injection
- XPATH Injection
- LDAP Injection
- Horizontal escalation of privileges (eg, accessing data of other patients or physicians)
- Vertical escalation of privileges (eg the access security context of a user in another profile, access account a patient at the doctor)
- Public vulnerabilities of type of common gateway interface (CGI)
- Public vulnerabilities of Common Gateway Interface (CGI)
- Inter-Domain Attacks (CSRF)
- Application-specific vulnerabilities (AJAX, Flash, ActiveX)
- The attacks of enumeration

Internal Infrastructure Pentest

Activitati:

- Reconnaissance (IP, DNS, Social Media, etc.)
- Testing firewall (firewalking, fragmentation, etc.)
- Discovery of the services – TCP/IP scanning, OS fingerprinting, banner grabbing, etc.
- Credentials hacking – enumeration, spraying, brute force, dictionary, mixed, etc.
- Google Hacking
- Specific vulnerability analysis systems in-scope
- Identifying vulnerabilities in the design
- Identifying vulnerabilities in the implementation / configuration
- Identifying vulnerabilities in the design and implementation of security policies
- Blackbox evaluation of design and implementation of VPN and remote access policies
- Exploitation of the specific vulnerabilities of externally exposed services
- Cracking of credentials using dictionary / brute-force / hybrid / spraying attacks
- MITM attempts, sniffing, spoofing
- Identification of backdoors, unsafe remote access gates
- DoS/DDoS amplification/logic bomb attacks

Teste de rezilienţă şi exemple de scenarii posibile:

Pentru a testa/îmbunătăți rezilienţa pot fi executate următoarele exemple de scenarii de testare sau pot fi dezvoltate scenarii personalizate în conformitate cu nevoile clientului.

- Defecţiunea dispozitivului/hardware-ului de reţea sau a maşinii virtuale:
- Testarea răspunsului sistemului (automate switching to a resilient resource) în caz de indisponibilitate a unei maşini fizice sau virtuale. Testul trebuie efectuat pe un activ convenit de comun acord de ambele părţi (client şi FORT).
- Atac de inginerie socială - propunem două scenarii de inginerie socială:
    - Pentru a colecta acreditările utilizatorilor folosind o platformă internă cunoscută ca ţintă – care va fi aleasă cu asistenţa clienţilor.
    - Simulare de atac de la un echipament mobil furat (laptop VIP pierdut/furat):

- Un laptop configurat în mod regulat pentru VIP cu utilizare extinsă a drepturilor de acces va fi folosit ca vector de atac într-un scenariu pierdut/furat, atunci când atacatorul nu știe nimic despre mașină (chei de acces, parole, nume de cont și chei de decriptare).
- Indisponibilitatea mediului de rezervă (pierdut/distrus):
  - Într-o situație de urgență, atunci când este nevoie de o copie de rezervă, echipa tehnică află că suportul de rezervă nu există sau nu este disponibil.
- Simulare de hacking extern:
  - Un atac de hacking extern extrem de puternic este simulat folosind un instrument de scanare agresiv extern pentru a afla cât de repede echipa internă de răspuns la incidente recunoaște "atacul" și ce măsuri de atenuare sunt luate.
- Comutarea activitatii Centrului operațional la site-ul secundar:
  - Testarea continuității operațiunilor zilnice presupunând indisponibilitatea Centrului Operațional Principal. Trecerea la site-ul secundar va fi efectuată manual de către administratorii clienților în afara orelor normale de lucru.

Metodologii pentru simulări de volume de tranzacții

1. Modelarea statistică a traficului

- Aplicarea variațiilor sezoniere și zilnice pentru a reflecta comportamentul real al utilizatorilor
- Includerea de anomalii controlate pentru testarea sistemelor de detecție

2. Generarea de trafic sintetic

- Crearea de seturi de date artificiale care mimează comportamentul real al utilizatorilor
- Implementarea de algoritmi de generare care respectă structura reală a tranzacțiilor
- Ajustarea parametrilor pentru a reprezenta diverse tipuri de companii și industrii

3. Replay-ul traficului istoric

- Utilizarea datelor reale anonimizate din sisteme de producție
- Scalarea volumului pentru a testa limita sistemelor de securitate
- Modificarea selectivă a tiparelor pentru a simula noi tipuri de amenințări

Activități specifice pentru simulări

Analiza și planificarea

- Definirea scopului simulării (testare de performanță, validare de algoritmi, etc.)
- Stabilirea indicatorilor de performanță care vor fi măsurați
- Identificarea scenariilor de simulare relevante pentru contextul specific

Implementarea tehnică

- Configurarea mediilor de testare izolate
- Dezvoltarea scripturilor pentru generarea și transmiterea tranzacțiilor
- Instrumentarea sistemelor pentru colectarea datelor de performanță

Execuția și monitorizarea

- Rularea simulărilor cu volume progresiv crescătoare
- Monitorizarea în timp real a comportamentului sistemelor
- Identificarea punctelor de eșec și a limitelor de performanță

Analiza rezultatelor

- Evaluarea performanței sistemelor de securitate sub diverse volume de tranzacții
- Identificarea corelațiilor între volume și rate de detectare/fals pozitive
- Formularea de recomandări pentru optimizarea sistemelor

Aceste metodologii și activități vor fi adaptate la sistemul BNM.

Metodologii pentru simulări de căderi de sistem și recuperare

1. Testarea de reziliență (Resilience Testing)

- Simularea planificată a defectării componentelor critice
- Implementarea de scenarii de dezastru în medii controlate
- Evaluarea capacității sistemelor de a-și menține funcționalitatea în condiții adverse

2. Chaos Engineering

- Injectarea controlată de defecte în sisteme în producție
- Crearea de perturbări aleatorii pentru a identifica vulnerabilitățile
- Testarea ipotezelor privind capacitatea sistemului de a rezista la evenimente neașteptate

3. Simularea de dezastre (Disaster Simulation)

- Crearea de scenarii complete de dezastru (incendii, inundații, atacuri cibernetice)
- Simularea căderii complete a centrelor de date sau infrastructurii
- Testarea planurilor de continuitate a afacerii (BCP) și recuperare după dezastru (DRP)

4. Failover și Failback Testing

- Testarea comutării automate între sisteme primare și secundare
- Verificarea proceselor de revenire la sistemele principale după remediere
- Evaluarea timpilor reali de recuperare comparativ cu obiectivele stabilite

Activități specifice pentru simulări

Planificare și pregătire

- Dezvoltarea scenariilor de cădere (hardware, software, rețea, atacuri cibernetice)
- Stabilirea obiectivelor de timp de recuperare (RTO) și punct de recuperare (RPO)
- Pregătirea echipelor și resurselor pentru exercițiile de recuperare

Implementare tehnică

- Configurarea instrumentelor de monitorizare și măsurare a performanței
- Implementarea mecanismelor de injectare a erorilor și defectelor
- Pregătirea sistemelor și datelor de backup pentru scenariile de recuperare

Execuția simulărilor

- Rularea exercițiilor de cădere în medii de test sau producție controlată
- Documentarea în timp real a comportamentului sistemelor și echipelor
- Implementarea procedurilor de recuperare conform planurilor documentate

Analiza post-exercițiu

- Evaluarea timpilor efectivi de detectare, răspuns și recuperare
- Identificarea punctelor slabe în procesele și sistemele de recuperare
- Documentarea lecțiilor învățate și a îmbunătățirilor necesare

Optimizarea continuă

- Actualizarea planurilor și procedurilor de recuperare
- Îmbunătățirea arhitecturii sistemelor pentru creșterea rezilienței
- Instruirea regulată a echipelor pe baza lecțiilor învățate

Exemple de scenarii specifice

- Simularea unei căderi complete a centrului de date principal
- Testarea restaurării sistemelor din backup-uri după un atac ransomware
- Simularea compromiterii credențialelor administrative și recuperarea controlului
- Testarea funcționalității sistemelor în cazul pierderii conectivității la rețea
- Simularea coruperii bazelor de date și testarea procedurilor de restaurare

Activități specifice pentru simulări DoS/DDoS

Testarea L4 (Transport Layer):

- Saturația rețelei, epuizarea lățimii de bandă, stresul firewall-ului / load balancer-ului.

Testarea L7 (Application layer):

- Performanța aplicațiilor web, baza de date, limitările resurselor serverului, vulnerabilitățile de nivel profund.

Evaluarea riscurilor DDoS

- Recunoaștere și revizuirea mediului: identificarea punctelor slabe pe care atacatorii le-ar putea exploata.
- Matricea amenințărilor: clasificarea impactului potențial pentru a prioritiza răspunsul.

Angajament deplin

- Alinierea înainte de testare: definirea de obiective clare și criterii de succes.
- Simulare și raportare a atacurilor: teste proactive "live-fire" cu monitorizare continuă a performanței.
- Asistență pentru remediere: recomandări practice pentru consolidarea apărării

Ca urmare a serviciilor prestate si descrise in capitolele A, B, C ale prezentei oferte, echipa FORT va furniza următoarele livrabile:

- Plan de proiect;
- Plan de analiză de riscuri/testare/audit;
- Planul de acțiuni (SOW – Scope of Work);
- Rapoartele privind analizele de riscuri trebuie să fie detaliate și să asigure acoperirea completă a domeniului soluției de plăți instant.
- Rapoarte care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor.
- Rapoarte de analiză, ce vor conține analiza rezultatelor testelor efectuate prin care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate.
- Raportul de audit va fi exhaustiv și va include, fără a se limita la: rezumatul executiv, scopul și obiectivele auditului, metodologia și standardele utilizate, observații și constatări, recomandări, probe de audit.
- Rapoarte de follow-up, ce va include evaluarea repetată riscurilor identificate în cadrul raportului primar și a eficienței măsurilor de control implementate

MIHAI PAJER EANU Date: 2025.08.04 18:14:52 +03'00'