ANEXA NR. 1

la Metodologie

EXEMPLE DE ACTIVITĂȚI AFERENTE PROCESULUI DE EVALUARE

1. Prezentăm în continuare o listă exemplificativă cu activități aferente procesului de evaluare:

a) verificarea analizei de conformitate;

b) verificarea analizei caracterului unitar;

c) examinarea eficienței mecanismelor de asigurare a securității;

d) examinarea vulnerabilităților constructive;

e) examinarea ușurinței de utilizare;

f) examinarea vulnerabilităților operaționale;

g) verificarea cerințelor;

h) verificarea proiectului de arhitectură a produsului;

i) verificarea proiectului detaliat;

j) verificarea implementării mecanismelor de asigurare a securității;

k) verificarea mediului de dezvoltare;

l) verificarea documentației de operare;

m) verificarea mediului operațional;

n) realizarea de teste de penetrare;

o) întocmirea raportului de evaluare.

2. Pentru claritate, precizăm că termenul de „verificare” implică analiza elementelor de evaluare, în timp ce „examinarea” furnizează date de intrare pentru realizarea testelor de penetrare. Deşi testele de penetrare sunt în mod explicit corelate cu activitățile anterioare, acestea au fost specificate ca şi activitate distinctă din două motive:

a) pentru a sublinia faptul că analizele anterioare trebuie consolidate şi apoi trebuie concepute testele, pe baza acestor analize;

b) pentru a indica faptul că, în general, diferitele teste de penetrare sunt realizate împreună.

3. Prin activitatea de verificare a analizei de conformitate, evaluatorul verifică analiza efectuată de dezvoltatorul produsului INFOSEC. Verificarea poate pune în evidență unele vulnerabilități rezultate, din cauza faptului că anumite funcții de securitate nu asigură atingerea unuia dintre obiectivele securității, în condițiile unei amenințări identificate în ținta de securitate.

4. Activitatea de verificare a analizei caracterului unitar constă în examinarea analizei efectuate de dezvoltatorul produsului INFOSEC şi stabileşte dacă setul de funcţii de securitate implementate, luate ca ansamblu, asigură în mod adecvat îndeplinirea obiectivelor securităţii.

5. Prin examinarea eficienţei mecanismelor de asigurare a securităţii, evaluatorul identifică eventualele mecanisme care nu ating eficienţa minimă cerută prin ţinta de securitate.

6. În procesul de examinare a vulnerabilităţilor rezultate din procesul de construcţie a produsului INFOSEC, evaluatorul trebuie să identifice eventuale astfel de vulnerabilităţi ale acestuia. Erorile identificate în procesul de evaluare a corectitudinii procesului de dezvoltare a produsului reprezintă o sursă de vulnerabilităţi constructive. Această activitate presupune examinarea erorilor, precum şi a diferitelor funcţionalităţi introduse în fiecare etapă a dezvoltării produsului.

7. Examinarea uşurinţei de utilizare presupune identificarea modurilor de operare nesigure a produsului INFOSEC. Prin urmare, această activitate este strâns legată de cerinţe operaţionale.

8. Activitatea de evaluare a vulnerabilităţilor operaţionale presupune ca evaluatorul să examineze modul de operare a produsului INFOSEC, pentru a identifica eventuale vulnerabilităţi apărute în cursul acestui proces.

9. Vulnerabilităţile operaţionale tratează aspecte la limita dintre măsurile de securitate IT şi cele non-IT, cum ar fi proceduri operaţionale privind securitatea fizică, modalităţi non-electronice de management al cheilor, distribuţia ecusoanelor de securitate etc. Măsurile de securitate non-IT trebuie să facă obiectul preocupărilor entităţii evaluatoare în următoarele situaţii:

a) apar ca parte a documentaţiei de operare;

b) ţinta de securitate este formulată pe baza unei politici de securitate a sistemului;

c) apar ca parte a documentaţiei produsului INFOSEC.

10. În procesul de analiză a vulnerabilităţilor operaţionale ale produsului INFOSEC, evaluatorii trebuie să analizeze dacă măsurile de securitate non-IT implementate contracarează vulnerabilităţile constructive identificate.

11. Activitatea de verificare a cerinţelor presupune ca evaluatorul să determine dacă ţinta de securitate defineşte în mod corect funcţiile care asigură implementarea securităţii. Ţinta de securitate trebuie să identifice clar aceste funcţii, nivelul de evaluare solicitat, precum şi măsurile de securitate implementate şi care trebuie avute în vedere în procesul de evaluare a produsului INFOSEC.

12. Prima etapă în procesul de dezvoltare a produsului, de la faza de cerinţe la cea de proiect de arhitectură, prezintă o importanţă deosebită, avându-se în vedere faptul că asigură corespondenţa

dintre funcțiile abstracte şi componentele logice şi fizice ale produsului INFOSEC. În acest context, una dintre principalele activități din procesul de evaluare este verificarea proiectului de arhitectură, în urma căreia evaluatorul decide dacă există o separare bine definită între funcționalitățile care asigură securitatea şi celelalte funcționalități ale produsului INFOSEC. În acest caz, activitatea de evaluare poate fi focalizată asupra elementelor care contribuie la asigurarea securității, iar ținta de securitate poate fi urmărită cu uşurință, pe măsură ce proiectul este analizat mai în detaliu.

13. Activitatea de verificare a proiectului detaliat presupune analiza modului în care este respectată politica privind separarea componentelor care asigură securitatea de celelalte componente, precum şi verificarea faptului că toate componentele care asigură implementarea securității sunt corect implementate.

14. Verificarea implementării presupune analiza modului în care sunt implementate mecanismele de asigurare a securității, într-un mod mai detaliat decât în cursul activității de verificare a proiectului. Analiza se bazează pe concluziile activității de verificare a proiectului detaliat, după care devine posibilă testarea funcțională.

15. Prin activitatea de verificare a mediului de dezvoltare se analizează în special standardele conform cărora este dezvoltat produsul. În cursul acestei activități se analizează:

a) controlul configurației;

b) limbajele de programare şi compilatoarele;

c) măsurile de securitate implementate de dezvoltator.

16. Activitatea de verificare a documentației de operare presupune verificarea faptului că produsul INFOSEC poate fi administrat şi utilizat în acord cu obiectivele sale de securitate.

17. Verificarea mediului de operare presupune ca evaluatorul să analizeze dacă produsul operațional este identic cu produsul rezultat din procesul de dezvoltare şi dacă acesta poate fi operat în conformitate cu obiectivele securității.

18. Testele de penetrare au rolul de a identifica eventuale vulnerabilități, care pot fi exploatate în procesul de utilizare a produsului INFOSEC.

19. Observațiile şi rezultatele fiecărei activități din procesul de evaluare trebuie consemnate în RTE.