BANCA NAȚIONALĂ A ROMÂNIEI

Cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO

Direcția Monitorizare a infrastructurilor pieței financiare și a plăților, octombrie 2022

Context internațional

În contextul geo-politic actual atacurile cibernetice sunt tot mai numeroase și mai sofisticate, cu un impact semnificativ, în special asupra instituțiilor financiare.

După atacuri majore ca cele asupra băncilor din Bangladesh și Valletta s-a relevat necesitatea unui cadru european de reglementare privind reziliența operațională digitală a sectorului financiar.

In anul 2018 Banca Centrală Europeană a elaborat cadrul pentru evaluarea și îmbunătățirea rezilienței cibernetice prin testarea reacției instituțiilor financiare la atacuri specifice grupărilor de crimă organizată și actorilor statali.

Despre TIBER

Threat Intelligence Based Ethical Red Teaming[1]

- Cadru de testare a rezilienței cibernetice, elaborat în 2018 la Banca Centrală Europeană, în cadrul Cyber Resilience Strategy Task Force.

- Transpus în legislația națională prin Regulamentul nr. 6/2022 privind cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO.

- Publicat în M.O. partea I, nr. 432/03.05.2022.

(1) https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

Domeniul de aplicare

- **Administratorii de infrastructuri ale pieței financiare** aflați în aria de monitorizare a Băncii Naționale a României;
- **Instituțiile de credit desemnate drept participanți critici** la infrastructurile pieței financiare.

Au obligația de a efectua teste de tip TIBER-RO cel puțin **o dată la 3 ani**.

Instituțiile de credit care nu sunt desemnate participanți critici, pot să efectueze teste de tip TIBER-RO în mod voluntar.

Entități testate

- **Administratorii de infrastructuri ale pieței financiare sunt:**
  - BNR-IPF - ReGIS, SaFIR; Transfond – SENT; Depozitarul central – RoClear

- **Instituțiile de credit desemnate drept participanți critici în 2022 sunt:**
  - ING Bank N.V., Amsterdam – Sucursala București; Raiffeisen Bank S.A.; Banca Comercială Română S.A.; UniCredit Bank S.A.; BRD – Groupe Société Générale S.A.; Citibank Europe p.l.c. Dublin - Sucursala România; Banca Transilvania S.A.

Caracteristici TIBER

TIBER este cadrul european de testare a rezilienței cibernetice, cu următoarele caracteristici:

- testul se realizează asupra infrastructurii de producție, procedurilor, personalului și serviciilor externalizate care susțin funcțiile critice ale entității testate;
- testarea se efectuează într-un mod controlat de către un furnizor de servicii de testare de tip *Ethical Red Teaming* care, pe baza raportului de tip *Cyber Threat Intelligence* specific entității testate, realizat de un furnizor de servicii de *Threat Intelligence*, simulează atacuri cibernetice de tip APT [1], cu scopul de a testa și îmbunătăți capacitățile de detecție și răspuns la incident, ale entității testate.

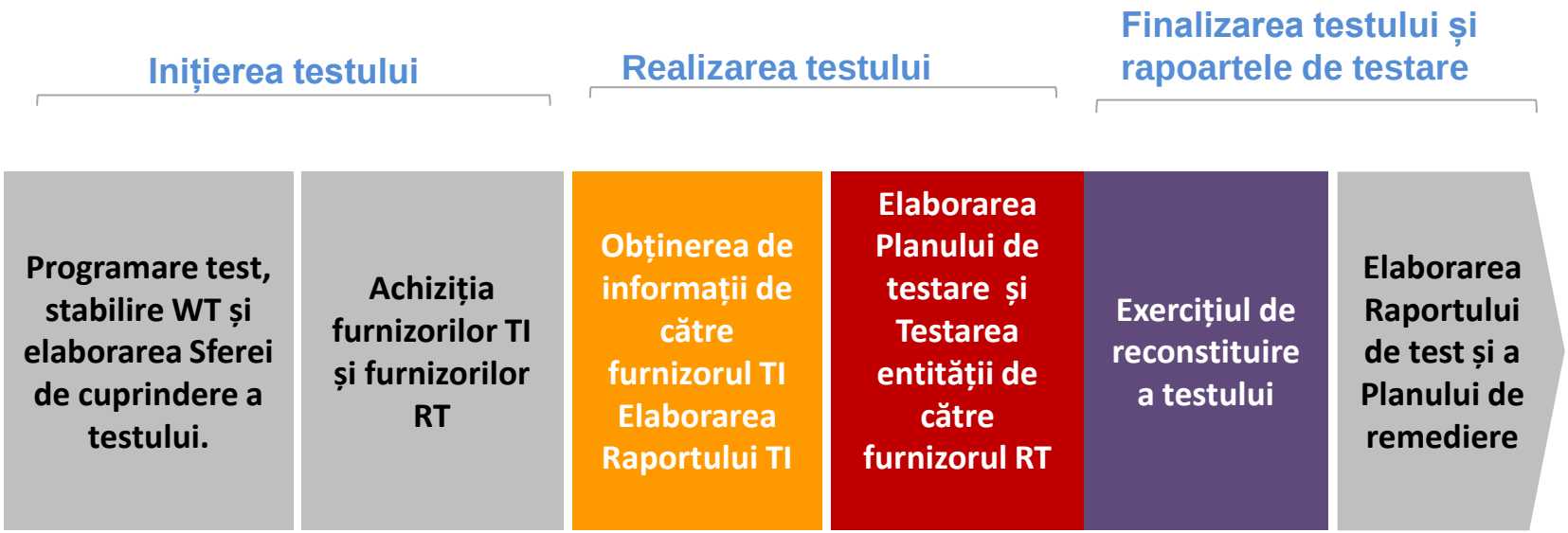
(1) Advanced Persistent Threats (APT) - este termenul folosit pentru a descrie o campanie de atac în care o echipă de intruși, stabilește o prezență ilegală, pe termen lung fără a fi detectată, în rețeaua țintă, pentru a îndeplini anumite obiective de atac.

TIBER-RO – părți implicate

BNR DMIPFP	Echipa Albă (White team) Entitatea testată (ET)	Furnizor TI (Threat Intelligence)	Furnizor RT (Red Team)	Echipa albastră (Blue Team) Entitatea testată
				
Monitorizează și atestă desfășurarea testului.	Gestionează desfășurarea testului.	Furnizează servicii de informații de tip *Cyber Threat Intelligence*.	Furnizează servicii de testare cibernetică.	Echipa de apărare din cadrul entității testate.

Echipa de reconstituire a testului (Purple Team)		Formată din reprezentanți ai RT și BT. Pot participa reprezentanți ai WT, TI și BNR.

Desfășurarea Testului TIBER-RO



TIBER-RO – Rolul BNR

BNR este implicată în toate fazele testului:

- Monitorizează testele pe tot parcursul desfășurării acestora;
- Furnizează îndrumare echipei albe (WT) pe toată durata desfășurării testului;
- Avizează întreaga documentație de testare;
- Atestă realizarea testării conform TIBER-RO;
- Monitorizează implementarea măsurilor cuprinse în Planul de remediere.

Cerințe pentru furnizorii de servicii TI și RT

- Furnizorii (la nivel de persoană juridică) trebuie să prezinte referințe de la instituții din domeniul financiar (3 pt. TI și 5 pt. RT) privind furnizarea unor servicii similare și să dispună de o asigurare de răspundere civilă în vigoare pentru activitățile desfășurate;
- Coordonatorul de echipă TI respectiv RT trebuie să dețină 5 ani de experiență profesională, din care cel puțin 3 ani în domeniul financiar, un Curriculum Vitae actualizat și cel puțin 3 referințe privind activitatea specifică, precum și o certificare cu una din calificările prevăzute la pct. III și pct. IV din Anexa nr. 2 din Regulamentul nr. 6/2022*;*
- Membrii echipelor TI respectiv RT trebuie să dețină 2 ani de experiență profesională, un Curriculum Vitae actualizat și o certificare cu una din calificările prevăzute la pct. IV din Anexa nr. 2 din Regulamentul nr. 6/2022*;*
- Echipele TI respectiv RT trebuie să aibă o compoziție multidisciplinară, vizând o gamă variată de abilități specifice.

III. Certificări ale coordonatorilor echipei TI sau ale coordonatorilor RT:

Organism de certificare	Calificarea
CREST	CREST Certified Threat Intelligence Manager (CCTIM)
CREST	CREST Certified Simulated Attack Manager (CCSAM)
Offensive Security	Offensive Security Certified Expert (OSCE)
eLearnSecurity	eLearnSecurity Certified Penetration Tester eXtreme (eCPTX)

IV. Calificări ale membrilor echipei TI sau ale membrilor RT:

Organism	Calificarea
CREST	CREST Certified Simulated Attack Specialist (CCSAS)
ISACA	CSX Penetration & Vulnerability Tester Pathway, CSX-P - Cybersecurity Practitioner Certification
(ISC)2	Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP)
SANS Institute - GIAC	GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Mobile Device Security Analyst (GMOB), GIAC Assessing and Auditing Wireless Networks (GAWN)
Offensive Security	Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Offensive Security Exploitation Expert (OSEE), Offensive Security Web Expert (OSWE)
eLearnSecurity	eLearnSecurity Certified Professional Penetration Tester (eCPPT), eLearnSecurity Web Application Penetration Tester (eWPT), eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX), eLearnSecurity Mobile Application Penetration Tester (eMAPT), eLearnSecurity Certified eXploit Developer (eCXD)
Altele	EC-Council Certified Security Analyst (ECSA), Licensed Penetration Tester (LPT), Certified Ethical Hacker (CEH)

DORA prevede teste TLPT[1]

Prin Regulamentul (UE) privind reziliența operațională digitală a sectorului financiar (DORA), în curs de finalizare, instituțiile financiare care operează în subsectoare care joacă un rol sistemic esențial (de exemplu plăți, servicii bancare, compensări și decontări) vor efectua, cel puțin o dată la 3 ani, teste de penetrare bazate pe amenințări (Threat-Led Penetration Testing - TLPT) în condiții asemănătoare testelor de tip TIBER.

(1) DORA *final compromise text*: https://data.consilium.europa.eu/doc/document/ST-10581-2022-INIT/en/pdf

Vă mulțumesc

Alexandru Dobrev

Șef serviciu

Direcția monitorizare a infrastructurilor pieței financiare și a plăților

BANCA NAȚIONALĂ A ROMÂNIEI

www.bnr.ro