TIBER-SK

Implementačný dokument

Jún 2025

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

www.nbs.sk

Vydavateľ

© Národná banka Slovenska Jún 2025

Odbor finančných technológií a inovácií

Adresa

Národná banka Slovenska
Imricha Karvaša 1
813 25 Bratislava
ITdohlad@nbs.sk

Obsah

Prehľad 4
TLPT v rámci zákona DORA 7
Ako súvisí regulačný technický predpis (RTS) o TLPT s rámcom TIBER-EÚ? 7
Ako súvisí program TIBER-SK s rámcom TIBER-EÚ a ďalšími implementáciami TIBER-XX? 7
Implementácia TIBER-SK 8
Orgán TLPT 8
TIBER Cyber Team (Tím TIBER pre kybernetickú bezpečnosť) 8
Cieľová skupina 9
Kontaktné údaje 9
Právne vyhlásenie 9
Príloha 10
Slovník pojmov 10
Hypertextové odkazy na TIBER-EÚ 11

Prehľad

TIBER-EÚ je rámcový program pre kybernetickú bezpečnosť, ktorý sa zameriava na simuláciu realistických kybernetických útokov na finančné subjekty (Financial Entities – FE). Na rozdiel od iných metodík rámec TIBER-EÚ umožňuje vykonávanie testov v reálnom prostredí na systémoch informačných a komunikačných technológií (IKT) (information and communication technology – ICT), ktoré zabezpečujú kritické alebo dôležité funkcie (Critical or Important Functions – CIF), procesy alebo osoby v rámci finančného subjektu bez nutnosti samostatného testovacieho prostredia, napríklad v produkčnom prostredí. Cieľom je neustále zlepšovať kybernetickú odolnosť celého finančného sektora a umožniť subjektu dosiahnuť vyššiu úroveň kybernetickej zrelosti.

TIBER-EÚ je rámec, ktorý vydala ECB v roku 2018 a bol aktualizovaný v roku 2025, aby zodpovedal požiadavkám zákona DORA. Centrum poznatkov TIBER-EÚ (Tiber Knowledge Centre – TKC) je fórum, ktoré prevádzkuje ECB a v rámci ktorého národné a európske kybernetické tímy TIBER koordinujú svoje aktivity, diskutujú o iniciatívach a zdieľajú zosumarizované informácie o svojich skúsenostiach.

Zákon o digitálnej prevádzkovej odolnosti (DORA) nadobudol účinnosť v roku 2025 a stanovil povinné červené tímové cvičenie, ktoré bolo podrobnejšie vysvetlené v regulačnom technickom predpise (Regulatory Technical Standard – RTS) o penetračnom testovaní na základe konkrétnej hrozby (Threat Led Penetration Testing – TLPT), ktorý bol publikovaný v tom istom roku. Aby sa predišlo fragmentácii, **Národná banka Slovenska (NBS) sa rozhodla implementovať rámec TIBER-EÚ.** Existuje množstvo národných usmernení (dokumentov) na zavedenie programu TIBER, pretože jurisdikcia v každej krajine zavedie program TIBER vo svojom národnom kontexte. Každá národná implementácia programu TIBER dodržiava rovnaké povinné požiadavky stanovené rámcom TIBER-EÚ.

TLPT rámca TIBER-SK je plne kompatibilné s požiadavkami rámca TIBER-EÚ a zákona DORA. Zákon **DORA ukladá určitým finančným subjektom (FE) povinnosť vykonať TLPT**. Subjekty, na ktoré sa nevzťahujú požiadavky zákona DORA na povinné TLPT, majú možnosť požiadať o dobrovoľný test TIBER. Dobrovoľný test môže byť naplánovaný podľa dostupnosti Slovenského tímu TIBER pre kybernetickú bezpečnosť (TIBER Cyber Team – TCT-SK). Finančné subjekty (FE), ktoré majú záujem o dobrovoľný test TIBER, musia mať primeranú úroveň kybernetickej zrelosti, preto je tento test zameraný na kritické a systémové inštitúcie na Slovensku.

Na teste TIBER-SK sa zúčastňuje viacero zainteresovaných strán. Finančný subjekt (FE) musí zriadiť kontrolný tím (Control Team – CT) pod vedením vedúceho kontrolného tímu (Control Team Lead – CTL), pričom iba členovia tohto tímu majú oprávnenie vedieť o prebiehajúcom teste TIBER-SK vo finančnom subjekte (s výnimkou prípadov, kedy je potrebné schválenie predstavenstvom). Modrý tím (Blue Team –BT) je zodpovedný za ochranu finančného subjektu (FE) a nesmie byť informovaný o teste. Orgán TLPT vyčlení testovacích manažérov (TM), aby sprevádzali finančný subjekt (FE) počas testovania. Poskytovateľ spravodajských informácií o hrozbách (Threat Intelligence Provider – TIP) musí byť externý poskytovateľ, ktorý vypracuje správy o spravodajských informáciách pre test a testovacie subjekty červeného tímu (Red Team Testers – RTT) uskutočnia útok na finančný subjekt (FE).

Finančný subjekt (FE) je zodpovedný za testovanie svojich systémov a zabezpečenie toho, aby z nich nevyplynulo žiadne riziko pre finančný subjekt alebo jeho zákazníkov. Náklady na test TLPT hradí finančný subjekt (FE), čo vyžaduje, aby subjekt zabezpečil adekvátne rozpočtové opatrenia.

Test TIBER-SK sa skladá z troch fáz: **Príprava**, **Testovanie** a **Záverečná fáza**.

Prípravná fáza sa začína, keď kontaktný bod vo vnútri **finančného subjektu (FE) dostane písomné oznámenie od orgánu TLPT**. Táto fáza zahŕňa štyri kroky: oznámenie, spustenie, určenie rozsahu pôsobnosti a obstarávanie. Vo fáze spustenia finančný subjekt (FE) zostaví kontrolný tím (CT), ktorý sa skladá z expertov, ktorí budú mať priamy prístup k predstavenstvu spoločnosti, ako aj dobrý prehľad o systémoch IKT v subjekte a o tretích stranách – dodávateľoch. Určenie rozsahu pôsobnosti a obstarávanie môžu prebiehať súbežne. Kontrolný tím (CT) musí vytvoriť dokumenty o spustení s popisom predbežných indikátorov na vysokej úrovni, vykonať počiatočné hodnotenie rizík a prijať príslušné opatrenia na minimalizáciu identifikovaných rizík. Táto fáza môže trvať až 6 mesiacov.

Po dokončení všetkých aktivít prípravnej fázy sa oficiálne spustí fáza testovania spolu s fázou poskytovania spravodajských informácií o hrozbách (threat intelligence – TI). Počas fázy poskytovania spravodajských informácií o hrozbách (TI) sa vytvorí viacero scenárov, z ktorých sa vyberú minimálne tri a vytvorí sa Cielená správa o spravodajských informáciách (Targeted Threat Intelligence Report – TTIR). Cielená správa o spravodajských informáciách (TTIR) podrobne vysvetľuje scenáre útokov z reálneho života, ktoré používajú kybernetickí protivníci, aby poskytla realistickú skúsenosť s hrozbami, ktoré predstavujú aktéri hrozieb. Táto fáza zvyčajne trvá 4 až 6 týždňov.

Po dokončení cielenej správy o spravodajských informáciách (TTIR) sa môže začať fáza červeného tímového cvičenia. Na základe cielenej správy o spravodajských informáciách (TTIR) testovací subjekt červeného tímu (RTT) vytvorí plán testu červeného tímu (Red Team Test Plan – RTTP), ktorý sa použije pri teste. Vo fáze aktívneho testovania sa testovací subjekt červeného tímu (RTT) pokúsi dosiahnuť vopred definované indikátory. **Toto je kritická fáza, ktorá prebieha na živých produkčných systémoch a trvá minimálne 12 týždňov.** Počas tejto fázy sa minimálne raz týždenne uskutočňujú stretnutia so všetkými príslušnými zainteresovanými stranami.

V záverečnej fáze bude modrému tímu (BT) oznámené, že prebehlo testovanie. Testovací subjekt červeného tímu (RTT) vypracuje vlastnú správu (RTTR), na základe ktorej bude vytvorená testovacia správa (BTTR) modrého tímu (BT). Všetky príslušné zainteresované strany budú mať možnosť zhodnotiť udalosti a poučiť sa z nich. Z tohto dôvodu sa uskutočňuje workshop s prehrávaním udalostí a fialové tímové cvičenie. Kontrolný tím (CT) po skončení vypracuje vytvorí súhrnnú správu o teste (Test Summary Report – TSR) a plán nápravy. Na záver sa uskutoční stretnutie, na ktorom si zainteresované strany vymenia spätnú väzbu. Záverečná fáza sa zvyčajne uskutoční v priebehu 18 týždňov.

Po úspešnom dokončení testu vydá orgán TLPT osvedčenie potvrdzujúce, že test bol vykonaný v súlade so základnými požiadavkami rámca TIBER-EÚ. Finančný subjekt (FE) musí vykonávať test TLPT každé tri roky, avšak orgán TLPT môže dĺžku tohto obdobia zmeniť.

TLPT v rámci zákona DORA

Nariadenie (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora v článku 26 ukladá povinné vykonávanie pokročilého penetračného testovania pre finančný subjekt (FE), ktorý je identifikovaný ako kritický alebo je potenciálne systémovo významný. Ďalšie usmernenia k tejto problematike nájdete v regulačnom technickom predpise zákona DORA pre penetračné testovanie založené na hrozbách.

Ako súvisí regulačný technický predpis (RTS) o TLPT s rámcom TIBER-EÚ?

Rámec TIBER-EÚ bol vyvinutý v spolupráci ECB a národných centrálnych bánk v rámci krajín EÚ, schválený Radou guvernérov ECB a publikovaný v máji 2018. Umožnil harmonizáciu testovania červených tímov v celej Európe a slúžil pre dobrovoľné testovanie TLPT finančného subjektu (FE).

Regulačný technický predpis (RTS) o TLPT bol vypracovaný na základe pôvodného rámca TIBER-EÚ. Medzi nimi však existovali drobné rozdiely. V roku 2025 bol rámec TIBER-EÚ zmenený a doplnený tak, aby bol plne v súlade s požiadavkami uvedenými v regulačnom technickom predpise (RTS).

TLPT je podľa zákona DORA právnym textom, ktorý určuje, **čo** je potrebné vykonať a aké sú právne požiadavky na proces, avšak nešpecifikuje presné postupy (napríklad stretnutia). Rámec TIBER-EÚ je špecifický vo svojich výstupoch a procesoch, ktoré je potrebné realizovať, opisuje **spôsob** vykonania testu. TIBER-EÚ tak predstavuje ideálnu príručku pre vykonávanie testov TLPT podľa zákona DORA.

Ako súvisí program TIBER-SK s rámcom TIBER-EÚ a ďalšími implementáciami TIBER-XX?

Jurisdikcia v každej krajine, ktorá sa rozhodne zaviesť rámec TIBER-EÚ, musí zverejniť národný dokument o implementácii. V súlade s týmto dokumentom NBS vyhlasuje, že všetky testy TIBER-SK budú vykonávané v súlade so štandardmi TIBER-EÚ.

Centrum poznatkov TIBER-EÚ je fórum, ktoré prevádzkuje ECB, kde národné a európske kybernetické tímy TIBER koordinujú svoje aktivity, diskutujú o iniciatívach a zdieľajú súhrnné informácie o svojich skúsenostiach. To pomáha zabezpečiť konzistentné vykonávanie rámca TIBER-EÚ v jurisdikciách štátov, ktoré ho preberajú.

K Jednotnému mechanizmu dohľadu existujú viaceré národné implementačné dokumenty, ako aj európska implementácia. Tieto dokumenty sa môžu líšiť v dĺžke a úrovni vysvetlenia procesov rámca TIBER-EÚ. Môžu tiež špecifikovať voliteľné prvky nad rámec TIBER-EÚ. V prípade spoločných testov TIBER sa príslušné orgány TLPT dohodnú na spôsobe implementácie, podľa ktorého budú postupovať (zvyčajne je to implementácia vedúceho orgánu TLPT).

Implementácia TIBER-SK

Všetky požiadavky rámca TIBER-EÚ sa priamo a úplne vzťahujú na implementáciu TIBER-SK. TIBER-SK neobsahuje žiadne odchýlky od rámca TIBER-EÚ. Úplné podrobnosti procesu testovania sú dostupné v rámci TIBER-EÚ. Celá dokumentácia rámca TIBER-EÚ je dostupná tu.

TIBER-EÚ umožňuje voliteľné kroky a pokiaľ ide o program TIBER-SK, sú akceptovateľné tieto:

Po vzájomnej dohode s testovacím manažérom (TM) môže finančný subjekt (FE) rozšíriť rozsah testu nad rámec kritických alebo dôležitých funkcií (CIF) a zapojiť ďalšie funkcie, procesy a tretie strany.

Fyzické červené tímové cvičenie pre test TLPT (napríklad utajené umiestnenie zariadenia v subjekte) je v rámci programu TIBER-SK povolené za predpokladu, že budú dodržané všetky potrebné bezpečnostné opatrenia.

Vytvorenie správy o všeobecnej panoráme hrozieb (Generic Threat Landscape – GTL Report) pre slovenský finančný sektor NIE JE garantované. Ak NBS vytvorí správu o všeobecnej panoráme hrozieb (GTL), informuje o tom finančný subjekt (FE) ihneď po oznámení, že správu je možné využiť na pomoc pri tvorbe cielenej správy o spravodajských informáciách (TTIR).

Orgán TLPT

Národná banka Slovenska je orgánom TLPT v Slovenskej republike. Zodpovedá za dobrovoľné aj povinné testy, ako aj testy pre významné inštitúcie (Significant institution – SI). Orgánom TLPT pre významné inštitúcie (SI) je ECB. ECB môže využiť národný TCT-SK na vykonanie povinného testu.

TIBER Cyber Team (Tím TIBER pre kybernetickú bezpečnosť)

Tím TLPT pre kybernetickú bezpečnosť, ako je definovaný v článku 3 regulačného technického predpisu (RTS) o TLPT, resp. tím TIBER pre kybernetickú bezpečnosť, ako je definovaný v kapitole 3.2 TIBER-EÚ (ďalej len TCT alebo TCT-SK), sídli v NBS ako stála pracovná skupina koordinovaná Odborom finančných inovácií.

TCT-SK pozostáva z testovacích manažérov (TM), ako je definované v článku 3 regulačného technického predpisu (RTS) o TLPT, respektíve v kapitole 3.3 rámca TIBER-EÚ. Testovací manažéri (TM) pochádzajú z viacerých divízií NBS, aby pokryli všetky typy inštitúcií tak, ako sú definované v článku 2 regulačného technického predpisu (RTS) o TLPT. Na každý test je vyčlenený jeden testovací manažér (TM) a aspoň jeden náhradný testovací manažér. Testovací manažéri (TM) a ich náhradní manažéri sú považovaní za rovnocenných.

V prípade testovania naprieč jurisdikciami jednotlivých štátov, najmä v kontexte cezhraničných situácií, môže TCT obsahovať pozorovateľov alebo testovacích manažérov z jurisdikcie iného štátu.

Cieľová skupina

Program TIBER-SK je zameraný na finančné subjekty (FE) poskytujúce svoje služby v rámci Slovenskej republiky, ktoré zohrávajú systémovú alebo významnú úlohu na slovenskom finančnom trhu. Finančný subjekt (FE) prijme všetky potrebné opatrenia na umožnenie účasti poskytovateľov služieb tretích strán v oblasti IKT na TLPT, ak poskytujú alebo podporujú kritické alebo dôležité funkcie (CIF) pre finančný subjekt (FE).

Orgán TLPT identifikuje finančné subjekty (FE), ktoré musia absolvovať povinné TLPT podľa článku 2 regulačného technického predpisu (RTS) o TLPT. Po úspešnom teste vydáva orgán TLPT osvedčenie. Osvedčenie o TLPT je zvyčajne platné 3 roky, avšak orgán TLPT môže toto obdobie predĺžiť alebo skrátiť.

Program TIBER-SK umožňuje dobrovoľné testovanie. Subjekty, ktoré majú záujem o dobrovoľné testovanie, sa môžu obrátiť na Národnú banku Slovenska. Na základe dostupných zdrojov TCT-SK NBS naplánuje test v spolupráci s finančným subjektom (FE).

Kontaktné údaje

V prípade otázok týkajúcich sa programu TIBER-SK alebo záujmu o dobrovoľný test sa obráťte na TCT-SK prostredníctvom e-mailu: ITdohlad@nbs.sk. TCT-SK čo najskôr odpovie na všetky otázky.

Všeobecné otázky týkajúce sa TIBER-EÚ môžete adresovať na ECB na e-mailovej adrese: tiber-eu@ecb.europa.eu. Otázky týkajúce sa významných inštitúcií (SI) môžete posielať TCT-SSM na e-mailovú adresu: tct-ssm@ecb.europa.eu

Právne vyhlásenie

Tento dokument predstavuje implementačnú dokumentáciu k rámcu TIBER-EÚ pre Slovenskú republiku (program TIBER-SK) a je určený výhradne na informačné účely. Informácie v tomto dokumente nie sú určené ako právne alebo iné odborné poradenstvo a nemali by byť považované za náhradu špecifického poradenstva prispôsobeného konkrétnym okolnostiam.

Finančný subjekt (FE), ktorý vykonáva test TIBER-SK, je výlučne zodpovedný za vykonanie úloh uvedených v tejto príručke, vrátane právneho a technického hodnotenia rizík (zahŕňajúceho dodržiavanie platných zákonov a predpisov) testu a príslušných bezpečnostných opatrení. NBS a ECB nenesú zodpovednosť za žiadne škody vzniknuté v dôsledku použitia tohto dokumentu alebo vykonávania testov TIBER-SK.

Terminológia použitá v tomto dokumente bola prevzatá z rámca TIBER-EÚ, nariadenia (EÚ) 2022/2554 a regulačných technických predpisov RTS zákona DORA týkajúcich sa TLPT (regulačné technické predpisy špecifikujúce prvky súvisiace s penetračným testovaním založeným na hrozbách podľa článku 26 ods. 11 nariadenia (EÚ) 2022/2554).

Príloha

Slovník pojmov

TKC	TIBER-EU Knowledge Centre (Centrum poznatkov TIBER-EÚ)
DORA	Digital Operational Resilience Act (Zákon o digitálnej prevádzkovej odolnosti)
RTS	Regulatory Technical Standards (Regulačné technické predpisy)
TLPT	Threat-Led Penetration Testing (Penetračné testovanie na základe konkrétnej hrozby
ICT (IKT)	Information and Communication Technology (Informačná a komunikačná technológia)
CIF	Critical or Important Functions (Kritické alebo dôležité funkcie)
FE	Financial Entities (Finančné subjekty)
SI	Significant Institution (Významná inštitúcia)
TCT	TIBER Cyber Team (Tím TIBER pre kybernetickú bezpečnosť)
TM	Test Manager (Testovací manažér)
CT	Control Team (Kontrolný tím)
CTL	Control Team Lead (Vedúci kontrolného tímu)
BT	Blue Team (Modrý tím)
TIP	Threat Intelligence Provider (Poskytovateľ spravodajských informácií o hrozbách)
RTT	Red Team Testers (Testovacie subjekty červeného tímu)
TI	Threat Intelligence (Spravodajské informácie o hrozbách)
GTL	Generic Threat Landscape (Všeobecná panoráma hrozieb)
RTTP	Red Team Test Plan (Plán testu červeného tímu)
TTIR	Targeted Threat Intelligence Report (Cielená správa o spravodajských informáciách)
RTTR	Red Team Test Report (Správa o teste červeného tímu)
BTTR	Blue Team Test Report (Správa o teste modrého tímu)
TSR	Test Summary Report (Súhrnná správa o teste)

Hypertextové odkazy na TIBER-EÚ

TIBER-EU framework (Rámec TIBER-EÚ)
TIBER-EÚ Control Team Guidance (Pokyny pre kontrolný tím TIBER-EÚ)
TIBER-EÚ Initiation Documents Guidance (Pokyny k dokumentom o spustení TIBER-EÚ)
TIBER-EU Guidance for Service Provider Procurement (Pokyny TIBER-EÚ pre obstarávanie poskytovateľov služieb)
TIBER-EU Scope Specification Template (Šablóna špecifikácie rozsahu TIBER-EÚ)
TIBER-EU Guidance for Target Threat Intelligence Report (Pokyny TIBER-EÚ pre cielenú správu o spravodajských informáciách)
TIBER-EU Red Team Test Plan Guidance (Pokyny TIBER-EÚ pre plán testu červeného tímu)
TIBER-EU Red Team Test Report Guidance (Pokyny TIBER-EÚ pre správu o teste červeného tímu)
TIBER-EU Blue Team Test Plan Guidance (Pokyny TIBER-EÚ pre plán testu modrého tímu)
TIBER-EU Purple Teaming Best Practices (Najlepšia prax TIBER-EÚ pre fialové tímové cvičenie)
TIBER-EU Guidance for the TIBER-EÚ Test Summary Report (Pokyny TIBER-EÚ pre súhrnnú správu o teste TIBER-EÚ)
TIBER-EU Remediation Plan Guidance (Pokyny TIBER-EÚ pre Plán nápravy)
TIBER-EU Attestation Guidance (Pokyny TIBER-EÚ pre osvedčenie)