Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1190

2025 6 18

KOMISIJOS DELEGUOTASIS REGLAMENTAS (ES) 2025/1190

2025 m. vasario 13 d.

kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 papildomas techniniais reguliavimo standartais, kuriais patikslinami kriterijai, naudojami finansų sektoriaus subjektams, kuriems būtina atlikti grėsmėmis grindžiamą skverbimosi testavimą, nustatyti, reikalavimai ir standartai, kuriais reglamentuojamas naudojimasis vidaus testuotojų paslaugomis, reikalavimai, susiję su grėsmėmis grindžiamo skverbimosi testavimo aprėptimi, testavimo metodika ir požiūriu, kurio reikia laikytis kiekvienu testavimo etapu, testavimo rezultatais, užbaigimu ir koregavimo etapais, taip pat bendradarbiavimo priežiūros srityje ir kitokio atitinkamo bendradarbiavimo, reikalingo atliekant grėsmėmis grindžiamą skverbimosi testavimą ir palengvinant tarpusavio pripažinimą, rūšimi

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 ([1]), ypač į jo 26 straipsnio 11 dalies ketvirtą pastraipą,

kadangi:

(1) šis reglamentas parengtas pagal sistemą TIBER-ES ir atspindi grėsmėmis grindžiamo skverbimosi testavimo (toliau – TLPT, angl. *threat-led penetration testing*) metodiką, procesą ir struktūrą, apibūdintus TIBER-ES. Finansų sektoriaus subjektai, kuriems būtina atlikti TLPT, gali remtis sistema TIBER-ES arba viena iš jos nacionalinių įgyvendinimo priemonių ir jas taikyti, jei ta sistema ar priemonės atitinka Reglamento (ES) 2022/2554 26 ir 27 straipsniuose ir šiame reglamente nustatytus reikalavimus. Vienos finansų sektoriaus valdžios institucijos, atsakingos už su TLPT susijusius klausimus nacionaliniu lygmeniu, paskyrimas pagal Reglamento (ES) 2022/2554 26 straipsnio 9 dalį neturėtų daryti poveikio Sąjungos lygmeniu kompetentingoms institucijoms suteiktai kompetencijai prižiūrėti tam tikrus finansų sektoriaus subjektus pagal to reglamento 46 straipsnį, pavyzdžiui, Europos Centrinio Banko kompetencijai prižiūrėti svarbias kredito įstaigas, kurios turi būti laikomos kompetentingomis su TLPT susijusių klausimų srityje. Jeigu pagal Reglamento (ES) 2022/2554 26 straipsnio 10 dalį kitai nacionalinei finansų sektoriaus institucijai perduodamos tik kai kurios su TLPT susijusios užduotys, to reglamento 46 straipsnyje nurodyto finansų sektoriaus subjekto kompetentinga institucija turėtų ir toliau būti institucija, kuri atsako už neperduotas su TLPT susijusias užduotis;

(2) atsižvelgiant į TLPT sudėtingumą ir su juo susijusią riziką, jį turėtų vykdyti tik tie finansų sektoriaus subjektai, kuriems jis yra pagrįstai reikalingas. Taigi už TLPT klausimus atsakingos institucijos (Sąjungos arba nacionalinio lygmens TLPT institucijos) į TLPT aprėptį neturėtų įtraukti tų finansų sektoriaus subjektų, kurie veikia pagrindinių finansinių paslaugų subsektoriuose ir kurių TLPT būtų nepagrįstas. Tai reiškia, kad kredito įstaigoms, mokėjimų ir elektroninių pinigų įstaigoms, centriniams vertybinių popierių depozitoriumams, pagrindinėms sandorių šalims, prekybos vietoms, draudimo ir perdraudimo įmonėms TLPT reikalavimas galėtų būti netaikomas, net jeigu šie subjektai ir atitinka kiekybinius kriterijus, atsižvelgiant į bendrą jų IRT rizikos profilio ir brandos, poveikio finansų sektoriui ir susijusių finansinio stabilumo problemų vertinimą;

(3) TLPT institucijos, atsižvelgdamos į bendrą IRT rizikos profilio ir brandos, poveikio finansų sektoriui ir susijusių finansinio stabilumo problemų vertinimą, turėtų įvertinti, ar TLPT reikalavimas turėtų būti taikomas kurios nors rūšies finansų sektoriaus subjektams, kurie nėra kredito įstaigos, mokėjimų įstaigos, elektroninių pinigų įstaigos, pagrindinės sandorių šalys, centriniai vertybinių popierių depozitoriumai, prekybos vietos, draudimo ir perdraudimo įmonės. Vertinant, ar tokie finansų sektoriaus subjektai atitinka tuos kokybinius kriterijus, turėtų būti siekiama naudojant tarpsektorinius ir objektyvius rodiklius nustatyti finansų sektoriaus subjektus, kuriems turėtų būti taikomas TLPT. Be to, vertinant, ar finansų sektoriaus subjektas atitinka tuos kokybinius kriterijus, TLPT reikalavimas turėtų būti taikomas tik tiems subjektams, kurių testavimas būtų pagrįstas. Tai, ar finansų sektoriaus

([1]) OL L 333, 2022 12 27, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

subjektas atitinka tuos kokybinius kriterijus, taip pat turėtų būti vertinama atsižvelgiant į naujus rinkų pokyčius ir į didėjančią naujų rinkos dalyvių, įskaitant kriptoturto paslaugų teikėjus, kuriems veiklos leidimai suteikiami pagal Europos Parlamento ir Tarybos reglamento (ES) 2023/1114 ([2]) 59 straipsnį, svarbą finansų sektoriui ateityje;

(4) finansų sektoriaus subjektai gali turėti tą patį IRT paslaugų teikėją grupės viduje arba priklausyti tai pačiai grupei ir naudoti bendras IRT sistemas. Tokiu atveju svarbu, kad TLPT institucijos, vertindamos, ar finansų sektoriaus subjektui turėtų būti taikomas TLPT reikalavimas ir ar TLPT turėtų būti atliekamas subjekto ar grupės lygmeniu (vykdant jungtinį TLPT), atsižvelgtų į to finansų sektoriaus subjekto struktūrą ir sisteminį pobūdį arba svarbą finansų sektoriui nacionaliniu ar Sąjungos lygmeniu;

(5) siekiant atspindėti sistemą TIBER-ES, būtina, kad testavimo metodikoje būtų numatomas šių pagrindinių subjektų dalyvavimas: finansų sektoriaus subjekto, turinčio kontrolės grupę (atitinkančią sistemos TIBER-ES kontrolės grupę) ir mėlynąją komandą (atitinkančią sistemos TIBER-ES mėlynąją komandą), ir TLPT institucijos, t. y. TLPT kibernetinės komandos (atitinkančios sistemos TIBER-ES TIBER kibernetinę komandą), žvalgybos informacijos apie grėsmes teikėjo ir testuotojų (testuotojai atitinka sistemos TIBER-ES raudonosios komandos paslaugų teikėją);

(6) siekiant užtikrinti, kad atliekant TLPT būtų galima išnaudoti patirtį, įgytą įgyvendinant sistemą TIBER-ES, ir sumažinti riziką, susijusią su TLPT vykdymu, turėtų būti užtikrinama, kad TLPT kibernetinių komandų, kurios turi būti sudaromos TLPT institucijų lygmeniu, pareigos kuo labiau atitiktų sistemos TIBER-ES kibernetinių komandų pareigas. Taigi turėtų būti paskiriami TLPT kibernetinių komandų testavimo vadovai, atsakingi už atskirų TLPT priežiūrą ir atskirų testų planavimą bei koordinavimą. TLPT kibernetinės komandos turėtų veikti kaip vienas bendras kontaktinis punktas su testavimu susijusiai komunikacijai su vidaus ir išorės suinteresuotaisiais subjektais vykdyti, grįžtamajai informacijai ir patirčiai, įgytai atliekant ankstesnius testus, kaupti ir tvarkyti, taip pat finansų sektoriaus subjektams, kuriems taikomas TLPT, remti;

(7) siekiant atspindėti sistemos TIBER-ES metodiką, testavimo vadovai turėtų turėti įgūdžių ir gebėjimų, kurių reikia, kad jie galėtų teikti konsultacijas ir ginčyti testuotojų pasiūlymus. Iš taikant sistemą TIBER-ES įgytos patirties matyti, kad naudinga kiekvienam testavimui paskirti ne mažiau kaip dviejų testavimo vadovų komandą. Atsižvelgiant į tai, kad TLPT naudojamas mokymosi patirčiai skatinti, ir siekiant užtikrinti testų konfidencialumą, TLPT institucijos (jeigu joms nekyla sunkumų dėl išteklių ar ekspertinių žinių) primygtinai raginamos užtikrinti, kad vykdant finansų sektoriaus subjekto TLPT, jo testavimo vadovai nevykdytų ir to paties finansų sektoriaus subjekto priežiūros veiklos;

(8) siekiant užtikrinti suderinamumą su sistema TIBER-ES, svarbu, kad TLPT institucija atidžiai stebėtų testavimą kiekviename jo etape. Atsižvelgiant į testavimo pobūdį ir su juo susijusią riziką, labai svarbu, kad TLPT institucija dalyvautų kiekviename konkrečiame testavimo etape. Visų pirma turėtų būti konsultuojamasi su TLPT institucija ir ji turėtų tvirtinti tuos finansų sektoriaus subjektų vertinimus ar sprendimus, kurie, viena vertus, gali turėti įtakos testo veiksmingumui ir, kita vertus, daryti poveikį su testu susijusiai rizikai. Pagrindiniai veiksmai, kuriuos atliekant turi konkrečiai dalyvauti TLPT institucija, yra tam tikrų esminių testavimo dokumentų tvirtinimas, žvalgybos informacijos apie grėsmes teikėjų ir testuotojų atranka ir rizikos valdymo priemonių nustatymas. TLPT institucijų dalyvavimas, visų pirma tvirtinimo tikslais, neturėtų tapti pernelyg didele našta toms institucijoms, todėl turėtų būti apsiribojama tik tais dokumentais ir sprendimais, kurie daro tiesioginį poveikį TLPT vykdymui. Aktyviai dalyvaudamos kiekviename testavimo etape TLPT institucijos gali veiksmingai įvertinti finansų sektoriaus subjektų atitiktį atitinkamiems reikalavimams, o šio vertinimo rezultatai turėtų padėti toms institucijoms išduoti pažymas pagal Reglamento (ES) 2022/2554 26 straipsnio 7 dalį;

([2]) 2023 m. gegužės 31 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1114 dėl kriptoturto rinkų, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1093/2010 bei (ES) Nr. 1095/2010 ir direktyvos 2013/36/ES bei (ES) 2019/1937 (OL L 150, 2023 6 9, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) siekiant užtikrinti, kad testavimo sąlygos būtų realistiškos, itin svarbus TLPT slaptumas. Todėl testavimas turėtų būti vykdomas slaptai ir turėtų būti imamasi atsargumo priemonių TLPT konfidencialumui užtikrinti, įskaitant kodinių pavadinimų, kurie turėtų būti kuriami taip, kad trečiosios šalys negalėtų atpažinti TLPT, parinkimą. Jeigu už finansų grupės saugumą atsakingi darbuotojai žinos apie planuojamą arba vykdomą TLPT, tikėtina, kad jie bus pastabesni ir budresni nei įprastomis darbo sąlygomis, todėl testavimo rezultatai gali būti kitokie. Dėl šios priežasties kontrolės grupei nepriklausantiems finansų sektoriaus subjekto darbuotojams apie planuojamą ar vykdomą TLPT turėtų būti pranešama tik esant nenuginčijamoms priežastims ir gavus išankstinį testavimo vadovų sutikimą, *inter alia*, siekiant užtikrinti testo slaptumą, jei mėlynosios komandos narys nustato, kad vykdomas testavimas;

(10) kaip matyti iš su kontrolės grupe susijusios patirties, įgytos taikant sistemą TIBER-ES, siekiant užtikrinti saugų TLPT atlikimą, būtina parinkti tinkamą kontrolės grupės vadovą. Kontrolės grupės vadovui turi būti suteikiami reikiami įgaliojimai finansų sektoriaus subjekte vadovauti visiems testavimo aspektams, nepakenkiant jo konfidencialumui. Dėl tos pačios priežasties kontrolės grupės nariai turėti išsamių žinių apie finansų sektoriaus subjektą, kontrolės grupės vadovo pareigas ir strateginę poziciją, būti įgiję reikiamą darbo stažą ir turėti galimybę bendrauti su valdyba. Siekiant užtikrinti TLPT sėkmę, kontrolės grupė turėtų būti kuo mažesnė;

(11) esama būdingų su TLPT susijusios rizikos elementų, nes ypatingos svarbos funkcijos išbandomos tikralaikėje produkcinėje aplinkoje, o dėl to gali kilti paslaugų trikdymo incidentų, atsirasti netikėtų sistemų gedimų, gali būti padaroma žala ypatingos svarbos tikralaikėms produkcijos sistemoms arba būti prarasti, pakeisti ar atskleisti duomenys. Šios rizikos rodo, kad reikia taikyti patikimas rizikos valdymo priemones. Siekiant užtikrinti, kad TLPT būtų kontroliuojamas viso testavimo metu, labai svarbu, kad finansų sektoriaus subjektai visada žinotų apie konkrečią vykdant TLPT kylančią riziką ir kad tą rizika būtų galima sumažinti. Šiuo atžvilgiu, nedarant poveikio finansų sektoriaus subjekto vidaus procesams ir kontrolės grupės vadovui jau priskirtoms atsakomybės sritims ir užduotims, gali būti tikslinga pateikti informaciją apie TLPT rizikos valdymo priemones arba tam tikrais atvejais tas rizikos valdymo priemones turėtų patvirtinti pats finansų sektoriaus subjekto valdymo organas. Siekiant teikti veiksmingas ir aukščiausios kvalifikacijos specialistų teikiamas paslaugas ir sumažinti šią riziką, taip pat labai svarbu, kad testuotojai ir žvalgybos informacijos apie grėsmes teikėjai (kartu – TLPT paslaugų teikėjai) turėtų aukščiausio lygio įgūdžių, ekspertinių žinių ir tinkamos patirties žvalgybos informacijos apie grėsmes teikimo ir TLPT finansinių paslaugų sektoriuje srityse;

(12) įprastiniai skverbimosi testai suteikia galimybę išsamiai ir naudingai įvertinti techninius ir konfigūracijos pažeidžiamumus, kurie dažnai būna susiję su viena sistema ar atskira aplinka, tačiau, kitaip nei atliekant žvalgybine informacija grindžiamą raudonosios komandos testavimą, juos atliekant nevertinamas visas tikslinio išpuolio prieš visą subjektą scenarijus, įskaitant visą jo žmonių, procesų ir technologijų aprėptį. Todėl TLPT paslaugų teikėjų atrankos proceso metu finansų sektoriaus subjektai turėtų užtikrinti, kad tie paslaugų teikėjai turėtų reikiamų įgūdžių ir galėtų vykdyti žvalgybos duomenimis grindžiamą raudonosios komandos testavimą, o ne tik skverbimosi testus. Taigi būtina nustatyti išsamius kriterijus, taikomus testuotojams (tiek vidaus, tiek išorės) ir žvalgybos informacijos apie grėsmes teikėjams, kurie visada yra išorės subjektai. Jeigu TLPT paslaugų teikėjai yra iš tos pačios bendrovės, TLPT vykdyti paskirti darbuotojai turėtų būti tinkamai atskiriami;

(13) gali būti išimtinių aplinkybių, kai finansų sektoriaus subjektai negali sudaryti sutarčių su išsamius kriterijus atitinkančiais TLPT paslaugų teikėjais. Todėl finansų sektoriaus subjektams, įrodžiusiems, kad tokie žvalgybos informacijos apie grėsmes teikėjai neprieinami, turėtų būti leidžiama įtraukti asmenis, kurie neatitinka visų išsamių kriterijų, su sąlyga, kad jie tinkamai sumažins bet kokią dėl to kylančią papildomą riziką ir kad visus tuos kriterijus įvertins TLPT institucija;

(14) jeigu vykdant TLPT dalyvauja keli finansų sektoriaus subjektai ir kelios TLPT institucijos, turėtų būti nurodomi visų TLPT proceso šalių vaidmenys, kad būtų galima atlikti veiksmingiausią ir saugiausią testą. Vykdant bendrą testavimą būtina nustatyti konkrečius reikalavimus, kad būtų galima apibrėžti paskirto finansų sektoriaus subjekto vaidmenį, t. y. kad jis turėtų būti atsakingas už visų būtinų dokumentų pateikimą pagrindinei TLPT institucijai ir už testavimo proceso stebėseną. Paskirtas finansų sektoriaus subjektas taip pat turėtų atsakyti už bendrus rizikos valdymo vertinimo aspektus. Nepaisant paskirto finansų sektoriaus subjekto vaidmens, atliekant bendrą testą neturėtų būti daromas poveikis kiekvieno finansų sektoriaus subjekto, dalyvaujančio bendro TLPT procese, pareigoms. To paties principo turėtų būti laikomasi ir vykdant jungtinį TLPT;

(15) kaip matyti iš sistemos TIBER-ES įgyvendinimo patirties, veiksmingiausias būdas užtikrinti tinkamą testavimą yra rengti fizinius arba virtualius susitikimus, kuriuose dalyvauja visi susiję suinteresuotieji subjektai (finansų sektoriaus subjektai, valdžios institucijos, testuotojai ir žvalgybos informacijos apie grėsmes teikėjai). Todėl įvairiais šio proceso etapais, visų pirma parengiamuoju etapu pradedant TLPT, ir siekiant galutinai susitarti dėl jo aprėpties testavimo etapu reikėtų rengti fizinius ir virtualius susitikimus, kad būtų baigta rengti žvalgybos informacijos apie grėsmes ataskaita ir raudonosios komandos testavimo planas ir kas savaitę informuojama apie padėtį. Šie susitikimai turėtų būti rengiami ir užbaigimo etapu, siekiant pakartoti testuotojų ir mėlynosios komandos veiksmus, vykdyti purpurinės komandos veiksmus ir keistis grįžtamąja informacija apie TLPT;

(16) siekdama užtikrinti sklandų TLPT vykdymą, TLPT institucija turėtų aiškiai nurodyti finansų sektoriaus subjektui savo lūkesčius, susijusius su testavimu. Šiuo atžvilgiu testavimo vadovai turėtų užtikrinti, kad būtų sukurtas tinkamas informacijos srautas tarp finansų sektoriaus subjekto kontrolės grupės ir TLPT paslaugų teikėjų;

(17) finansų sektoriaus subjektas turėtų pasirinkti ypatingos svarbos arba svarbias funkcijas, kurios bus tikrinamos vykdant TLPT. Atrinkdamas tas funkcijas, finansų sektoriaus subjektas turėtų remtis įvairiais kriterijais, susijusiais su kiekvienos funkcijos svarba pačiam finansų sektoriaus subjektui ir finansų sektoriui Sąjungos ir nacionaliniu lygmenimis ne tik ekonominiu požiūriu, bet ir atsižvelgiant į simbolinį ar politinį tam tikros funkcijos statusą. Kad būtų lengviau sklandžiai pereiti į žvalgybos informacijos apie grėsmes rinkimo etapą, kontrolės grupė turėtų pateikti testuotojams ir žvalgybos informacijos apie grėsmes teikėjui, kurie nedalyvauja aprėpties nustatymo procese, išsamią informaciją apie sutartą aprėpties nustatymą;

(18) siekiant testuotojams suteikti informaciją, reikalingą tikrojo laiko ir tikroviškam išpuoliui prieš finansų sektoriaus subjekto tikralaikes sistemas, kuriomis grindžiamos jo ypatingos svarbos ar svarbios funkcijos, imituoti, žvalgybos informacijos apie grėsmes teikėjas turėtų rinkti žvalgybos informaciją arba informaciją, apimančią bent dvi pagrindines interesų sritis: taikinius, nustatant galimus išpuolio perimetrus visame finansų sektoriaus subjekte, ir grėsmes, nustatant atitinkamus grėsmę keliančius subjektus ir galimus grėsmės scenarijus. Siekiant užtikrinti, kad žvalgybos informacijos apie grėsmes teikėjas atsižvelgtų į atitinkamas grėsmes finansų sektoriaus subjektui, testuotojai, kontrolės grupė ir testavimo vadovai turėtų pateikti grįžtamąją informaciją dėl žvalgybos informacijos apie grėsmes ataskaitos projekto. Jei turima, žvalgybos informacijos apie grėsmes teikėjas kaip nacionalinės grėsmių aplinkos atskaitos tašku gali remtis TLPT institucijos valstybės narės finansų sektoriui pateikta bendra grėsmių panorama. Remiantis sistemos TIBER-ES taikymo patirtimi, žvalgybos informacijos apie grėsmes rinkimo procesas paprastai trunka maždaug keturias savaites;

(19) siekiant užtikrinti, kad testuotojai galėtų gauti įžvalgų ir toliau peržiūrėti aprėpties aprašymą ir tikslinės žvalgybos informacijos apie grėsmes ataskaitą ir tuomet būtų galima užbaigti raudonosios komandos testavimo planą, labai svarbu, kad prieš TLPT raudonosios komandos testavimo etapą testuotojai iš žvalgybos informacijos apie grėsmes teikėjo gautų išsamius paaiškinimus dėl tikslinės žvalgybos informacijos apie grėsmes ataskaitos ir galimų grėsmių scenarijų analizės;

(20) siekiant užtikrinti, kad testuotojai galėtų atlikti realistiškus ir išsamius testus, kurių metu vykdomi visi išpuolių etapai ir nustatomos grėsmės, reikėtų skirti pakankamai laiko aktyviojo raudonosios komandos testavimo etapui. Remiantis taikant sistemą TIBER-ES įgyta patirtimi, turėtų būti skiriamas bent 12 savaičių laikotarpis ir jis turėtų būti nustatomas atsižvelgiant į dalyvaujančių šalių skaičių, TLPT aprėptį, susijusio (-ių) finansų sektoriaus subjekto (-ų) išteklius, išorės reikalavimus ir finansų sektoriaus subjekto pateiktos patvirtinamosios informacijos prieinamumą;

(21) aktyviojo raudonosios komandos testavimo etapu testuotojai turėtų taikyti įvairią taktiką, metodus ir procedūras, kad būtų galima tinkamai išbandyti finansų sektoriaus subjekto tikralaikes produkcijos sistemas. Taktika, metodai ir procedūros turėtų, kai tinkama, apimti iššvalgymą (siekiant surinkti kuo daugiau informacijos apie taikinį), instrumentalizavimą (t. y. informacijos apie infrastruktūrą, įrenginius ir darbuotojus analizę ir pasirengimą su konkrečiu taikiniu susijusioms operacijoms), atlikimą (t. y. visos taikiniui taikomos operacijos aktyvavimą), išnaudojimą (tais atvejais, kai testuotojų tikslas yra užvaldyti finansų sektoriaus subjekto serverius, tinklus ir išnaudoti jo darbuotojus pasitelkiant socialinę inžineriją), kontrolę ir judėjimą (t. y. pastangas pereiti nuo užvaldytų sistemų prie kitų pažeidžiamų ar didelės vertės sistemų) ir taikiniui taikomus veiksmus (t. y. siekiant dar geresnės prieigos prie užvaldytų sistemų ir prieigos prie tikslinės informacijos ir duomenų, dėl kurių anksčiau buvo susitarta raudonosios komandos testavimo plane);

(22) atlikdami TLPT testuotojai turėtų atsižvelgti į laiką, skirtą išpuoliui įvykdyti, išteklius ir etines bei teisines ribas. Jei testuotojai negali pereiti į kitą užprogramuotą išpuolio etapą, TLPT institucijai sutikus kontrolės grupė kartkartėmis turėtų teikti pagalbines paslaugas. Tokios pagalbinės paslaugos iš esmės gali būti skirstomos į informacijos ir prieigos kategorijas ir gali apimti prieigos prie IRT sistemų ar vidaus tinklų suteikimą, kad būtų galima toliau vykdyti testavimą ir sutelkti dėmesį į tolesnius išpuolio etapus;

(23) aktyviojo etiško įsilaužimo testavimo metu, jei būtina, kad būtų galima toliau vykdyti TLPT, kaip kraštutinė priemonė išskirtinėmis aplinkybėmis ir išnaudojus visas alternatyvias galimybes turėtų būti vykdoma bendradarbiaujamoji testavimo veikla, kurioje dalyvautų ir testuotojai, ir mėlynoji komanda. Atliekant tokius ribotus purpurinės komandos veiksmus, galima taikyti šiuos metodus: „sugauti ir paleisti“, kai testuotojai stengiasi toliau veikti pagal scenarijus, yra aptinkami ir po to toliau vykdo testavimą; „karo žaidynės“, kai sudaromos sąlygos sudėtingesniems scenarijams siekiant išbandyti strateginių sprendimų priėmimą, arba „bendradarbiaujamasis koncepcijos įrodymas“, kai testuotojams ir mėlynosios komandos nariams suteikiama galimybė kontroliuojamoje ir bendradarbiavimo aplinkoje bendrai patvirtinti konkrečias saugumo priemones, įrankius ar metodus;

(24) TLPT turėtų būti naudojamas kaip mokymosi patirtis siekiant didinti finansų sektoriaus subjektų skaitmeninės veiklos atsparumą. Šiuo atžvilgiu mėlynoji komanda ir testuotojai turėtų pakartoti išpuolį ir, bendradarbiaudami su testuotojais, peržiūrėti veiksmus, siekdami pasimokyti iš testavimo patirties. Tuo tikslu ir siekiant užtikrinti tinkamą pasirengimą, prieš pradedant bet kokią pakartojimo veiklą visoms pakartojant išpuolį dalyvaujančioms šalims turėtų būti suteikiama galimybė susipažinti su raudonosios komandos testavimo ataskaita ir mėlynosios komandos testavimo ataskaita. Be to, siekiant kuo labiau išnaudoti mokymosi patirtį, užbaigimo etapu turėtų būti atliekami purpurinės komandos veiksmai. Metodai, kurie gali būti naudojami atliekant purpurinės komandos veiksmus užbaigimo etape, turėtų apimti alternatyvių išpuolių scenarijų aptarimą, alternatyvių scenarijų tikralaikių sistemų tyrimą arba pakartotinį planuojamų scenarijų, susijusių su tikralaikėmis sistemomis, kurių testuotojai negalėjo užbaigti arba įvykdyti testavimo etapu, išnagrinėjimą;

(25) siekiant sudaryti dar palankesnes sąlygas visoms TLPT dalyvaujančioms šalims įgyti mokymosi patirties, kuri būtų naudinga atliekant testavimą ateityje, ir didinti finansų sektoriaus subjektų skaitmeninės veiklos atsparumą, atitinkamos šalys turėtų teikti viena kitai grįžtamąją informaciją apie visą procesą ir visų pirma nustatyti, kurie veiksmai vyko tinkamai arba kuriuos reikėtų patobulinti, ir kurie TLPT proceso aspektai buvo tinkami arba kuriuos reikėtų patobulinti;

(26) Reglamento (ES) 2022/2554 46 straipsnyje nurodytos kompetentingos institucijos ir TLPT institucijos (jeigu jos ne tos pačios) turėtų bendradarbiauti, siekdamos į esamus priežiūros procesus įtraukti pažangius TLPT metodus. Šiuo atžvilgiu ir siekiant teisingai suprasti TLPT rezultatus bei tai, kaip jie turėtų būti aiškinami, tikslinga, kad, visų pirma rengiant apibendrinamąją testavimo ataskaitą ir koregavimo planus, TLPT dalyvavę testavimo vadovai ir atsakingos priežiūros institucijos glaudžiai bendradarbiautų;

(27) Reglamento (ES) 2022/2554 26 straipsnio 8 dalies pirmoje pastraipoje reikalaujama, kad finansų sektoriaus subjektai kas trečiam testui atlikti sudarytų sutartis su išorės testuotojais. Jeigu finansų sektoriaus subjektai į testuotojų grupę įtraukia tiek vidaus, tiek išorės testuotojus, turėtų būti laikoma, kad toks testavimas yra TLPT, to straipsnio taikymo tikslais atliekamas kartu su vidaus testuotojais;

(28) šis reglamentas grindžiamas techninių reguliavimo standartų projektais, kuriuos Komisijai pateikė Europos bankininkystės institucija, Europos draudimo ir profesinių pensijų institucija ir Europos vertybinių popierių ir rinkų institucija (Europos priežiūros institucijos), gavusios Europos Centrinio Banko pritarimą;

(29) Europos priežiūros institucijos dėl techninių reguliavimo standartų projektų, kuriais grindžiamas šis reglamentas, surengė atviras viešas konsultacijas, išnagrinėjo galimas susijusias išlaidas ir naudą ir paprašė Bankininkystės suinteresuotųjų šalių grupės, įsteigtos pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 1093/2010 ([3]) 37 straipsnį, Draudimo ir perdraudimo suinteresuotųjų subjektų grupės ir Profesinių pensijų suinteresuotųjų subjektų grupės, įsteigtų pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 1094/2010 ([4]) 37 straipsnį, ir Vertybinių popierių ir rinkų suinteresuotųjų šalių grupės, įsteigtos pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 1095/2010 ([5]) 37 straipsnį, pateikti savo nuomonę;

(30) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 42 straipsnio 1 dalimi ([6]), buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis 2024 m. rugpjūčio 20 d. pateikė nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) kontrolės grupė – grupė, kurioje dirba testuojamo finansų sektoriaus subjekto darbuotojai ir, kai aktualu atsižvelgiant į TLPT aprėptį, jam paslaugas teikiančių trečiųjų šalių ir bet kurios kitos testą valdančios šalies darbuotojai;

2) kontrolės grupės vadovas – finansų sektoriaus subjekto darbuotojas, atsakingas už visos su finansų sektoriaus subjekto TLPT susijusios veiklos vykdymą, atliekant konkretų testą;

3) mėlynoji komanda – finansų sektoriaus subjekto darbuotojai ir, kai aktualu, finansų sektoriaus subjektui paslaugas teikiančių trečiųjų šalių ir bet kurios kitos šalies, kuri, atsižvelgiant į TLPT aprėptį, laikoma svarbia, darbuotojai, saugantys finansų sektoriaus subjekto naudojamus tinklus ir informacines sistemas, padėdami išlaikyti tokią jo kibernetinio saugumo būklę, kad būtų galima apsisaugoti nuo imituojamų ar realių išpuolių, ir nežinantys, kad vykdomas TLPT;

4) mėlynosios komandos užduotys – užduotys, kurias įprastai atlieka mėlynoji komanda, pavyzdžiui, saugumo operacijų centro (SOC) funkcijos, IRT infrastruktūros paslaugos, pagalbos tarnybos paslaugos, incidentų valdymo paslaugos operacijų lygmeniu;

5) raudonoji komanda – vidaus ar išorės testuotojai, kuriems pagal sutartis patikėta arba kurie paskiriami atlikti TLPT;

6) purpurinės komandos veiksmai – bendradarbiaujamoji testavimo veikla, kurią vykdant dalyvauja ir testuotojai, ir mėlynoji komanda;

([3]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB, (OL L 331, 2010 12 15, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1094/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/79/EB, (OL L 331, 2010 12 15, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1095/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) ir iš dalies keičiamas Sprendimas Nr. 716/2009/EB bei panaikinamas Komisijos sprendimas 2009/77/EB, (OL L 331, 2010 12 15, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) TLPT institucija – bet kuri iš šių institucijų:

   a) viena finansų sektoriaus valdžios institucija, paskirta pagal Reglamento (ES) 2022/2554 26 straipsnio 9 dalį;

   b) finansų sektoriaus institucija, kuriai pagal Reglamento (ES) 2022/2554 26 straipsnio 10 dalį pavesta vykdyti kai kurias arba visas su TLPT susijusias užduotis;

   c) bet kuri Reglamento (ES) 2022/2554 46 straipsnyje nurodyta kompetentinga institucija;

8) TLPT kibernetinio saugumo grupė – TLPT institucijų darbuotojai, atsakingi už su TLPT susijusius klausimus;

9) testavimo vadovai – darbuotojai, paskirti vadovauti su konkrečiu TLPT susijusiems TLPT institucijos veiksmams ir stebėti, kaip laikomasi šio reglamento;

10) žvalgybos informacijos apie grėsmes teikėjas – ekspertai, kuriuos finansų sektoriaus subjektas pasamdo kiekvienam TLPT atlikti ir kurie nėra finansų sektoriaus subjekto ir grupės vidaus IRT paslaugų teikėjai (jei tokių yra), kurie renka ir analizuoja tikslinę žvalgybos informaciją apie grėsmes, susijusią su finansų sektoriaus subjektais, kuriuos apima konkretus TLPT, ir kuria atitinkamus ir realistiškus grėsmių scenarijus;

11) TLPT paslaugų teikėjai – testuotojai ir žvalgybos informacijos apie grėsmes teikėjai;

12) pagalbinės paslaugos – kontrolinės grupės teikiama pagalba arba informacija testuotojams, kad jie galėtų toliau vykdyti išpuolio kelią, kai patys negali daryti pažangos ir kai nėra kitos pagrįstos alternatyvos, be kita ko, dėl nepakankamo laiko ar išteklių vykdant tam tikrą TLPT;

13) išpuolio kelias – trajektorija, kuria TLPT aktyviojo raudonosios komandos testavimo etapu veikia testuotojai, siekdami sukelti tam TLPT nustatytas grėsmes;

14) grėsmės – pagrindiniai uždaviniai, susiję su grėsmėmis IRT sistemoms, kuriomis palaikomos ypatingos svarbos arba svarbios finansų sektoriaus subjekto funkcijos, kurias testuotojai stengiasi sukelti testavimo metu;

15) neskelbtina informacija – informacija, kuria galima lengvai pasinaudoti vykdant išpuolius prieš finansų sektoriaus subjekto IRT sistemas, intelektinė nuosavybė, konfidencialūs verslo duomenys arba asmens duomenys, kurie gali tiesiogiai ar netiesiogiai pakenkti finansų sektoriaus subjektui ir jo ekosistemai, jei jie patektų į piktavališkų subjektų rankas;

16) bendro testavimo dalyviai – visi finansų sektoriaus subjektai, dalyvaujantys atliekant bendrą TLPT pagal Reglamento (ES) 2022/2554 26 straipsnio 4 dalį;

17) priimančioji valstybė narė – priimančioji valstybė narė pagal kiekvienam finansų sektoriaus subjektui taikomą Sąjungos sektorių teisę;

18) jungtinis TLPT – TLPT, išskyrus bendrą TLPT, kaip nurodyta Reglamento (ES) 2022/2554 26 straipsnio 4 dalyje, kurį atliekant dalyvauja keli finansų sektoriaus subjektai, besinaudojantys to paties grupės vidaus IRT paslaugų teikėjo paslaugomis arba priklausantys tai pačiai grupei ir naudojantys bendras IRT sistemas.

2 straipsnis

Finansų sektoriaus subjektų, kuriems būtina atlikti TLPT, nustatymas

1. TLPT institucijos įvertina, ar kuriam nors finansų sektoriaus subjektui būtina atlikti TLPT, atsižvelgdamos į tų finansų sektoriaus subjektų poveikį, jų sisteminį pobūdį ir IRT rizikos profilį, remdamosi visais toliau išvardytais kriterijais:

a) su poveikiu ir sisteminiu pobūdžiu susiję veiksniai:

   i) finansų sektoriaus subjekto dydis, nustatytas remiantis tuo, ar finansų sektoriaus subjektas teikia finansines paslaugas vienoje ar daugiau valstybių narių, ir palyginus finansų sektoriaus subjekto veiklą su kitų panašias paslaugas teikiančių finansų sektoriaus subjektų veikla;

   ii) finansų sektoriaus subjekto tarpusavio sąsajų su kitais finansų sektoriaus subjektais vienoje ar daugiau valstybių narių mastas ir pobūdis;

   iii) paslaugų, kurias finansų sektoriaus subjektas teikia finansų sektoriui, ypatinga svarba arba svarbumas;

iv) finansų sektoriaus subjekto teikiamų paslaugų pakeičiamumas;

v) finansų sektoriaus subjekto verslo modelio ir susijusių paslaugų bei procesų sudėtingumas;

vi) ar finansų sektoriaus subjektas priklauso sisteminio pobūdžio grupei, veikiančiai finansų sektoriuje Sąjungos ar nacionaliniu lygmeniu ir naudojančiai bendras IRT sistemas;

b) su IRT rizika susiję veiksniai:

i) finansų sektoriaus subjekto rizikos profilis;

ii) finansų sektoriaus subjekto grėsmių panorama;

iii) finansų sektoriaus subjekto ypatingos svarbos ar svarbių funkcijų arba jas palaikančių funkcijų priklausomumo nuo IRT sistemų ir procesų mastas;

iv) finansų sektoriaus subjekto IRT struktūros sudėtingumas;

v) IRT paslaugos ir funkcijos, kurias palaiko IRT paslaugas teikiančios trečiosios šalys, ir sutartimis įformintų susitarimų su IRT paslaugas teikiančiomis trečiosiomis šalimis arba grupės vidaus IRT paslaugų teikėjais skaičius ir rūšys;

vi) bet kokių priežiūrinių tikrinimų, susijusių su finansų sektoriaus subjekto IRT brandos įvertinimu, rezultatai;

vii) IRT veiklos tęstinumo planų ir IRT reagavimo ir veiklos atkūrimo planų branda;

viii) grėsmių operacinių IRT saugumui aptikimo ir mažinimo priemonių branda, įskaitant gebėjimą:

1) nuolat stebėti finansų sektoriaus subjekto IRT infrastruktūrą;

2) tikruoju laiku nustatyti su IRT susijusius įvykius;

3) analizuoti 2 punkte nurodytus įvykius;

4) laiku ir veiksmingai reaguoti į 2 punkte nurodytus įvykius;

ix) ar finansų sektoriaus subjektas priklauso grupei, veikiančiai finansų sektoriuje Sąjungos ar nacionaliniu lygmeniu ir naudojančiai bendras IRT sistemas.

Taikydama a punkto i papunktį, TLPT institucija, kai įmanoma, atsižvelgia į:

a) finansų sektoriaus subjekto rinkos dalį Sąjungos ir nacionaliniu lygmenimis;

b) finansų sektoriaus subjekto siūlomos veiklos spektrą;

c) finansų sektoriaus subjekto teikiamų paslaugų arba Sąjungos ir nacionaliniu lygmenimis vykdomos veiklos rinkos dalį.

Taikydama a punkto v papunktį, TLPT institucija, kai įmanoma, atsižvelgia į:

a) tai, ar finansų sektoriaus subjektas veikia pagal daugiau nei vieną verslo modelį;

b) įvairių verslo procesų ir susijusių paslaugų tarpusavio sąsajas.

2. TLPT institucijos turi reikalauti, kad TLPT vykdytų visi toliau nurodyti finansų sektoriaus subjektai, išskyrus atvejus, kai iš 1 dalyje nurodyto finansų sektoriaus subjekto vertinimo matyti, kad dėl šio subjekto poveikio, su juo susijusių finansinio stabilumo problemų arba IRT rizikos profilio jo dalyvavimas atliekant TLPT nebūtų pateisinamas:

a) kredito įstaigos, kurios atitinka bet kurią iš šių sąlygų:

i) nustatyta, kad pagal Europos Parlamento ir Tarybos direktyvos 2013/36/ES ([7]) 131 straipsnį jos yra pasaulinės sisteminės svarbos įstaigos (G-SII);

ii) nustatyta, kad pagal Europos Parlamento ir Tarybos direktyvos 2013/36/ES 131 straipsnį jos yra kitos sisteminės svarbos įstaigos (O-SII);

iii) jos priklauso G-SII arba O-SII;

([7]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB, (OL L 176, 2013 6 27, p. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) mokėjimo įstaigos, kurių bendra mokėjimo operacijų, apibrėžtų Europos Parlamento ir Tarybos direktyvos (ES) 2015/2366 ([8]) 4 straipsnio 5 punkte, vertė kiekvienais iš dvejų kalendorinių metų iki TLPT institucijos atlikto vertinimo viršijo 150 mlrd. EUR;

c) elektroninių pinigų įstaigos, kurių bendra mokėjimo operacijų, apibrėžtų Direktyvos (ES) 2015/2366 4 straipsnio 5 punkte, vertė kiekvienais iš dvejų kalendorinių metų iki TLPT institucijos atlikto vertinimo viršijo 150 mlrd. EUR arba kurių bendra neapmokėtų elektroninių pinigų suma viršijo 40 mlrd. EUR;

d) centriniai vertybinių popierių depozitoriumai;

e) pagrindinės sandorių šalys;

f) prekybos vietos, kuriose veikia elektroninė prekybos sistema, atitinkančios bet kurį iš šių kriterijų:

i) prekybos vietai tenka didžiausia rinkos dalis pagal bet kurio iš toliau nurodytų produktų apyvartą nacionaliniu lygmeniu kiekvienais iš dvejų kalendorinių metų iki TLPT institucijos atlikto vertinimo:

1) perleidžiamųjų vertybinių popierių, apibrėžtų Europos Parlamento ir Tarybos direktyvos 2014/65/ES 4 straipsnio 1 dalies 44 punkto a papunktyje ([9]);

2) perleidžiamųjų vertybinių popierių, apibrėžtų Europos Parlamento ir Tarybos direktyvos 2014/65/ES 4 straipsnio 1 dalies 44 punkto b papunktyje;

3) išvestinių finansinių priemonių, apibrėžtų Europos Parlamento ir Tarybos reglamento (ES) Nr. 600/2014 ([10]) 2 straipsnio 1 dalies 29 punkte;

4) struktūrizuotų finansinių produktų, apibrėžtų Reglamento (ES) Nr. 600/2014 2 straipsnio 1 dalies 28 punkte;

5) apyvartinių taršos leidimų, kaip nurodyta Direktyvos 2014/65/ES I priedo C skirsnio 11 punkte;

ii) prekybos vietai tenkanti rinkos dalis pagal bet kurio iš toliau nurodytų produktų apyvartą Sąjungos lygmeniu kiekvienais iš dvejų kalendorinių metų iki TLPT institucijos atlikto vertinimo viršija 5 %:

1) bendrovių akcijų ir kitų vertybinių popierių, lygiaverčių bendrovių, ūkinių bendrijų ar kitų subjektų akcijoms, bei depozitoriumo pakvitavimų dėl akcijų;

2) obligacijų ir kitos formos skolos vertybinių popierių, įskaitant depozitoriumo pakvitavimus, susijusius su tokiais vertybiniais popieriais;

3) išvestinių finansinių priemonių, apibrėžtų Reglamento (ES) Nr. 600/2014 2 straipsnio 1 dalies 29 punkte;

4) struktūrizuotų finansinių produktų, apibrėžtų Reglamento (ES) Nr. 600/2014 2 straipsnio 1 dalies 28 punkte;

5) apyvartinių taršos leidimų, kaip nurodyta Direktyvos 2014/65/ES I priedo C skirsnio 11 punkte;

([8]) 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB, (OL L 337, 2015 12 23, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES, (OL L 173, 2014 6 12, p. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 600/2014 dėl finansinių priemonių rinkų, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012, (OL L 173, 2014 6 12, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) draudimo ir perdraudimo įmonės, atitinkančios visus toliau nurodytus kriterijus:

i) jų bendra pasirašytų įmokų suma viršija 1 500 000 000 EUR;

ii) jų techniniai atidėjiniai viršija 10 000 000 000 EUR;

iii) draudimo įmonės, kurios vykdo tik gyvybės draudimo veiklą arba vykdo ir gyvybės, ir ne gyvybės draudimo veiklą ir kurių bendras turtas viršija 3,5 % viso valstybėje narėje įsteigtų draudimo ir perdraudimo įmonių turto, įvertinto pagal Europos Parlamento ir Tarybos direktyvos 2009/138/EB ([11]) 75 straipsnį, sumos.

Taikant f punkto ii papunktį, kai prekybos vieta priklauso grupei, kurioje naudojamos bendros IRT sistemos arba naudojamasi to paties IRT grupės vidaus paslaugų teikėjo paslaugomis, turi būti atsižvelgiama į vertybinių popierių ir išvestinių finansinių priemonių sutarčių apyvartą visose tai pačiai grupei priklausančiose ir Sąjungoje įsisteigusiose prekybos vietose.

Taikant g punktą, TLPT institucijos turi nustatyti visų draudimo ir perdraudimo įmonių pogrupį, vadovaudamosi g punkto i, ii ir iii papunkčiuose nustatytais kriterijais. Tam pogrupiui priskirtos draudimo ir perdraudimo įmonės turi atlikti TLPT, jei jos taip pat atitinka bet kurį iš šių kriterijų:

a) bendra pasirašytų įmokų suma viršija 3 000 000 000 EUR;

b) techniniai atidėjiniai viršija 30 000 000 000 EUR;

c) bendra turto suma viršija 10 % valstybėje narėje įsteigtų draudimo ir perdraudimo įmonių bendros turto sumos, įvertintos pagal Direktyvos 2009/138/EB 75 straipsnį.

3. Jeigu daugiau nei vienas tai pačiai grupei priklausantis ir bendras IRT sistemas naudojantis finansų sektoriaus subjektas arba daugiau nei vienas to paties grupės viduje veikiančio IRT paslaugų teikėjo paslaugomis besinaudojantis finansų sektoriaus subjektas atitinka 2 dalyje nustatytus kriterijus, tų finansų sektoriaus subjektų TLPT institucijos pagal 16 straipsnio 2 dalį turi nuspręsti, ar reikalavimas atlikti atskirą TLPT yra aktualus tiems finansų sektoriaus subjektams.

Jeigu pirmoje pastraipoje nurodytos finansų sektoriaus subjektų grupės patronuojančiosios įmonės TLPT institucija nėra viena iš grupės finansų sektoriaus subjektų TLPT institucijų, tai grupei priklausančių finansų sektoriaus subjektų TLPT institucijos turi konsultuotis su ta institucija dėl to, ar tikslinga vykdyti atskirą TLPT.

3 straipsnis

Kibernetinio saugumo grupė ir TLPT testavimo vadovai

1. TLPT institucija atsakomybę už su TLPT susijusios veiklos koordinavimą priskiria kibernetinio saugumo grupei. Kibernetinio saugumo grupę sudaro testavimo vadovai, paskirti prižiūrėti atskirą TLPT.

2. TLPT institucija paskiria kiekvieno testavimo vadovą ir bent vieną atsarginį vadovą.

3. Testavimo vadovai stebi, ar laikomasi šiame reglamente nustatytų reikalavimų, ir užtikrina, kad jų būtų laikomasi.

([11]) 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II) (OL L 335, 2009 12 17, p. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Testavimo vadovas 9 straipsnio 1 dalyje nurodytu pranešimu pateikia finansų sektoriaus subjektui kibernetinio saugumo grupės kontaktinius duomenis.

5. TLPT institucija dalyvauja visuose TLPT etapuose.

4 straipsnis

Su finansų sektoriaus subjektais susiję organizaciniai aspektai

1. Finansų sektoriaus subjektai paskiria kontrolės grupės vadovą, kuris atsako už kasdieninį TLPT valdymą ir kontrolės grupės sprendimus bei veiksmus.

2. Finansų sektoriaus subjektai nustato organizacines ir procedūrines priemones, kuriomis užtikrinama, kad:

a) galimybė susipažinti su informacija, susijusia su planuojamu ar vykdomu TLPT, pagal principą „būtina žinoti“ būtų suteikiama tik kontrolės grupei, valdymo organui, testuotojams, žvalgybos informacijos apie grėsmes teikėjui ir TLPT institucijai;

b) prieš įtraukdama bet kurį mėlynosios komandos narį į TLPT veiksmus, kontrolės grupė tartųsi su testavimo vadovais;

c) kontrolės grupei būtų pranešama apie bet kokį atvejį, kai finansų sektoriaus subjektas arba jam paslaugas teikiančių trečiųjų šalių darbuotojai aptinka TLPT; paaštrėjus atsakui į incidentus, prireikus kontrolės grupė jį suvaldytų;

d) būtų sudaromi susitarimai dėl TLPT slaptumo, kurių turi laikytis finansų sektoriaus subjekto darbuotojai, atitinkamų IRT paslaugas teikiančių trečiųjų šalių darbuotojai, testuotojai ir žvalgybos informacijos apie grėsmes teikėjas;

e) gavusi prašymą, kontrolės grupė testavimo vadovams pateiktų visą su TLPT susijusią informaciją;

f) kai įmanoma, minėdamos TLPT, jame dalyvaujančios šalys naudotų tik kodinį pavadinimą.

5 straipsnis

TLPT rizikos valdymas

1. 9 straipsnyje nurodytu parengiamuoju etapu kontrolės grupė įvertina riziką, susijusią su finansų sektoriaus subjekto ypatingos svarbos arba svarbių funkcijų tikralaikių produkcijos sistemų testavimu, įskaitant galimą poveikį:

a) finansų sektoriui;

b) finansiniam stabilumui Sąjungos arba nacionaliniu lygmeniu.

Kontrolės grupė tą poveikį turi tikrinti visą testavimo laikotarpį.

2. Rizikos vertinimo ir valdymo tikslais kontrolės grupė turi atsižvelgti bent į šių rūšių riziką, susijusią su:

a) galimybe žvalgybos informacijos apie grėsmes teikėjui ir išorės testuotojams susipažinti su neskelbtina informacija apie finansų sektoriaus subjektą (kai aktualu);

b) Reglamento (ES) 2022/2554 ir šio reglamento nuostatų neatitinkančiu TLPT, kai dėl tokio neatitikimo neišduodama Reglamento (ES) 2022/2554 26 straipsnio 7 dalyje nurodyta pažyma, įskaitant atvejus, kai reikalavimų nesilaikoma dėl TLPT konfidencialumo pažeidimų arba neetiško elgesio;

c) krizių ir incidentų eskalavimu;

d) aktyviuoju raudonosios komandos etapu, įskaitant riziką, susijusią su ypatingos svarbos veiklos nutraukimu ir duomenų sugadinimu dėl testuotojų veiklos, ir galimą poveikį trečiosioms šalims;

e) mėlynosios komandos veikla, įskaitant riziką, susijusią su ypatingos svarbos veiklos nutraukimu ir duomenų sugadinimu dėl mėlynosios komandos veiklos, ir galimą poveikį trečiosioms šalims;

f) neužbaigtu atliekant TLPT paveiktų sistemų atkūrimu.

6 straipsnis

Bendro arba jungtinio TLPT rizikos valdymas

1. Atliekant jungtinį arba bendrą TLPT kiekvieno finansų sektoriaus subjekto kontrolės grupė atlieka savo rizikos vertinimą ir nustato savo rizikos valdymo priemones.

2. Šio reglamento 16 straipsnio 3 dalies b punkte nurodyto paskirto finansų sektoriaus subjekto arba pagal Reglamento (ES) 2022/2554 26 straipsnio 4 dalį paskirto finansų sektoriaus subjekto kontrolės grupė įvertina riziką, susijusią su kelių finansų sektoriaus subjektų dalyvavimu atliekant TLPT. Dalyvaujančių finansų sektoriaus subjektų kontrolės grupės bendradarbiauja su paskirto finansų sektoriaus subjekto kontrolės grupe ir nustato galimą bendrą riziką.

7 straipsnis

TLPT paslaugų teikėjų atranka

1. Kontrolės grupė imasi priemonių su TLPT susijusiai rizikai valdyti ir visų pirma užtikrina, kad atliekant kiekvieną TLPT:

a) žvalgybos informacijos apie grėsmes teikėjas ir išorės testuotojai kontrolės grupei pateiktų išsamius gyvenimo aprašymus ir sertifikatų, kurie pagal pripažintus rinkos standartus yra tinkami jų veiklai vykdyti, kopijas;

b) žvalgybos informacijos apie grėsmes teikėjas ir išorės testuotojas būtų tinkamai ir visiškai apdrausti atitinkamu profesinės civilinės atsakomybės draudimu, įskaitant draudimą nuo netinkamo elgesio ir aplaidumo rizikos;

c) žvalgybos informacijos apie grėsmes teikėjas nurodytų bent tris anksčiau įgyvendintus projektus, susijusius su skverbimosi testavimu ir raudonųjų komandų testavimu;

d) išorės testuotojai nurodytų bent penkis anksčiau įgyvendintus projektus, susijusius su skverbimosi testavimu ir raudonųjų komandų testavimu;

e) vykdyti TLPT paskirti žvalgybos informacijos apie grėsmes teikėjo darbuotojai:

i) būtų bent vadovas, turintis ne mažiau kaip penkerių metų žvalgybos informacijos apie grėsmes teikimo patirtį, ir bent vienas papildomas narys, turintis ne mažiau kaip dvejų metų žvalgybos informacijos apie grėsmes teikimo patirtį;

ii) turėtų įvairių ir tinkamo lygio profesinių žinių ir įgūdžių, įskaitant:

1) žinias apie žvalgybos informacijos rinkimo taktiką, metodus ir procedūras;

2) geopolitines, technines ir su sektoriais susijusias žinias;

3) tinkamus bendravimo įgūdžius, kad galėtų aiškiai pristatyti veiklos rezultatus ir apie juos informuoti;

iii) bendrai būtų dalyvavę ne mažiau kaip trijose ankstesnėse užduotyse, susijusiose su žvalgybos informacija apie grėsmes, teikiama atliekant skverbimosi testavimą ir raudonosios komandos testavimą;

iv) tuo pat metu nevykdytų jokių mėlynosios komandos užduočių ar neteiktų kitų paslaugų, dėl kurių gali kilti interesų konfliktas, susijęs su TLPT, kuriam jie yra priskirti, dalyvaujančiu finansų sektoriaus subjektu, IRT paslaugas teikiančia trečiąja šalimi ar grupės vidaus IRT paslaugų teikėju;

v) būtų atskirti nuo TLPT paslaugų teikėjo, parūpinančio išorės testuotojus tam pačiam TLPT atlikti, darbuotojų ir nebūtų jiems pavaldūs;

f) jeigu tai išorės testuotojai, TLPT paskirta raudonoji komanda:

i) būtų bent vadovas, turintis ne mažiau kaip penkerių metų skverbimosi testavimo ir raudonųjų komandų testavimo patirtį, ir bent du papildomi testuotojai, kiekvienas turintis ne mažiau kaip dvejų metų skverbimosi testavimo ir raudonųjų komandų testavimo patirtį;

ii) turėtų įvairių ir tinkamo lygio profesinių žinių ir įgūdžių, įskaitant žinias apie finansų sektoriaus subjekto veiklą, iššvalgymą, rizikos valdymą, spragų išnaudojimo priemonių kūrimą, fizinį įsiskverbimą, socialinę inžineriją, pažeidžiamumo analizę, taip pat tinkamus bendravimo įgūdžius, kad galėtų aiškiai pristatyti veiklos rezultatus ir apie juos pranešti;

iii) bendrai būtų dalyvavusi ne mažiau kaip penkiose ankstesnėse užduotyse, susijusiose su skverbimosi testavimu ir raudonųjų komandų testavimu;

iv) nebūtų žvalgybos informacijos apie grėsmes teikėjo, kuris vienu metu teikia mėlynosios komandos paslaugas finansų sektoriaus subjektui, IRT paslaugas teikiančiai trečiajai šaliai arba grupės vidaus IRT paslaugų teikėjui, kurie dalyvauja atliekant TLPT, darbuotojas ir neteiktų jiems paslaugų;

v) būtų atskirta nuo bet kurių to paties TLPT paslaugų teikėjo, kuris tuo pačiu metu teikia žvalgybos informacijos apie grėsmes paslaugas atliekant tą patį TLPT, darbuotojų;

g) baigę testavimą testuotojai ir žvalgybos informacijos apie grėsmes teikėjas atlieka atkūrimo procedūras, įskaitant saugų informacijos, susijusios su slaptažodžiais, kredencialais ir kitais slaptais raktais, kuriems atliekant TLPT buvo sukeltas pavojus, pašalinimą, saugų pranešimą finansų sektoriaus subjektams apie paskyras, kurioms buvo sukeltas pavojus, bei saugų testuojant surinktų kitų duomenų rinkimą, saugojimą, valdymą ir pašalinimą;

h) testuotojai atlieka ne tik atkūrimo procedūras baigus testavimą, nurodytas g punkte, bet ir toliau nurodytas atkūrimo procedūras:

i) komandų ir kontrolės priemonių deaktyvavimas;

ii) aprėpties ir datų avarinis stabdymas (angl. *kill switches*);

iii) užpakalinių durų ir kitos kenkimo programinės įrangos pašalinimas;

iv) pranešimas apie galimus pažeidimus;

v) būsimo atsarginio atkūrimo procedūros, kurios gali būti susijusios su kenkimo programine įranga ar testavimo metu įdiegtomis priemonėmis;

vi) mėlynosios komandos veiklos stebėsena ir kontrolės grupės informavimas apie galimus aptikimo atvejus;

i) testuotojai ir žvalgybos informacijos apie grėsmes teikėjai nevykdo toliau nurodytos veiklos ir joje nedalyvauja:

i) neteisėtas finansų sektoriaus subjekto ir jam IRT paslaugas teikiančių trečiųjų šalių, jei tokių yra, įrangos sunaikinimas;

ii) nekontroliuojamas finansų sektoriaus subjekto ir jam IRT paslaugas teikiančių trečiųjų šalių, jei tokių yra, informacijos ir IRT turto pakeitimas;

iii) tyčinis pakenkimas finansų sektoriaus subjekto ypatingos svarbos arba svarbių funkcijų tęstinumui;

iv) neleistinas pagal testavimo aprėptį nenumatytų sistemų įtraukimas;

v) neleistinas bandymų rezultatų atskleidimas.

2. Kontrolės grupė registruoja testuotojų ir žvalgybos informacijos apie grėsmes teikėjų pateiktus dokumentus, kuriais įrodoma atitiktis 1 dalies a–f punktams.

Išskirtinėmis aplinkybėmis finansų sektoriaus subjektai gali sudaryti sutartis su išorės testuotojais ir žvalgybos informacijos apie grėsmes teikėjais, kurie neatitinka vieno ar daugiau iš 1 dalies a–f punktuose nustatytų reikalavimų, su sąlyga, kad tie finansų sektoriaus subjektai imasi tinkamų priemonių rizikai, susijusiai su tokių punktų nesilaikymu, sumažinti ir tas priemones užregistruoja.

8 straipsnis

Bendro arba jungtinio TLPT ypatumai

1. Jeigu pagrindinė TLPT institucija nenusprendžia kitaip, tais atvejais, kai atliekant bendrą arba jungtinį TLPT dalyvauja keli finansų sektoriaus subjektai, nustatomi pagal 16 straipsnio 2 arba 4 dalį, kiekvienas finansų sektoriaus subjektas turi atlikti visus 9–15 straipsniuose nustatytus veiksmus.

2. Jeigu šiame reglamente numatyta kitaip, kai jungtiniame TLPT arba bendrame TLPT dalyvauja kelios TLPT institucijos, kaip nurodyta 16 straipsnio 3 arba 5 dalyje, 9–15 straipsniuose nuorodos į TLPT instituciją turi būti suprantamos kaip nuorodos į tokio bendro arba jungtinio TLPT pagrindinę instituciją.

9 straipsnis

Parengiamasis etapas

1. Pagal Reglamento (ES) 2022/2554 26 straipsnio 8 dalies trečią pastraipą nustatytas finansų sektoriaus subjektas TLPT inicijuoja gavęs TLPT institucijos pranešimą, kad reikia atlikti TLPT.

2. Per tris mėnesius nuo 1 dalyje nurodyto pranešimo gavimo finansų sektoriaus subjektas testavimo vadovams pateikia visą toliau nurodytą TLPT inicijavimo informaciją:

a) projekto aprašymą, įskaitant aukšto lygio projekto planą, kuriame pateikiama I priede nurodyta informacija;

b) kontrolės grupės vadovo kontaktinius duomenis;

c) informaciją apie tai, kad planuojama naudotis vidaus ir (arba) išorės testuotojų paslaugomis, kaip nurodyta 15 straipsnyje;

d) informaciją apie ryšių kanalus, kurie bus naudojami atliekant TLPT;

e) TLPT kodinį pavadinimą.

3. Jeigu 2 dalies a–e punktuose nurodyta informacija yra išsami ir ja užtikrinamas TLPT tinkamumas ir veiksmingas vykdymas, TLPT institucija patvirtina finansų sektoriaus subjekto TLPT inicijavimo informaciją ir apie tai praneša finansų sektoriaus subjektui.

4. TLPT institucijai patvirtinus TLPT inicijavimo informaciją, finansų sektoriaus subjektas sudaro kontrolės grupę, kuri padeda kontrolės grupės vadovui atlikti šias užduotis:

a) nustatyti kontrolės grupės ryšių su testuotojais ir žvalgybos informacijos apie grėsmes teikėjais kanalus ir procesus, kurie turi būti naudojami visais su TLPT susijusiais klausimais;

b) informuoti finansų sektoriaus subjekto valdymo organą apie TLPT pažangą ir susijusią riziką;

c) viso TLPT metu priimti ekspertinėmis žiniomis grindžiamus sprendimus;

d) vykdyti TLPT laikantis šio reglamento nuostatų;

e) parinkti TLPT žvalgybos informacijos apie grėsmes teikėją;

f) parinkti išorės ir (arba) vidaus testuotojus;

g) parengti aprėpties aprašymą.

5. Jeigu TLPT institucija mano, kad pradinė kontrolės grupės sudėtis ir bet kokie vėlesni jos pakeitimai yra tinkami 4 dalyje nurodytoms užduotims atlikti, TLPT institucija patvirtina kontrolės grupę ir apie tai praneša kontrolės grupės vadovui.

6. Per 6 mėnesius nuo 1 dalyje nurodyto TLPT institucijos pranešimo gavimo finansų sektoriaus subjektas testavimo vadovams pateikia aprėpties aprašymą, kuriame pateikiama visa II priede nurodyta informacija. Aprėpties aprašymą patvirtina finansų sektoriaus subjekto valdymo organas.

7. Finansų sektoriaus subjektai, siekdami į TLPT aprėptį įtraukti ypatingos svarbos ar svarbias funkcijas, atsižvelgia į šiuos kriterijus:

a) funkcijos ypatingą svarbumą ar svarbą ir galimą jos poveikį finansų sektoriui ir finansiniam stabilumui Sąjungos ir nacionaliniu lygmenimis;

b) funkcijos svarbą finansų sektoriaus subjekto kasdienei verslo veiklai;

c) funkcijos pakeičiamumą;

d) tarpusavio sąsajas su kitomis funkcijomis;

e) funkcijos geografinę padėtį;

f) kitų sektoriaus subjektų priklausomybę nuo funkcijos;

g) jei įmanoma, su funkcija susijusią žvalgybos informaciją apie grėsmes.

8. Sudariusi sutartis su testuotojais ir žvalgybos informacijos apie grėsmes teikėjais, kontrolės grupė turi pasidalyti su jais TLPT inicijavimo informacija ir aprėpties aprašymu. Kontrolės grupė informuoja testuotojus ir žvalgybos informacijos apie grėsmes teikėjus apie testavimo procesą, kurio reikia laikytis.

9. Finansų sektoriaus subjektas užtikrina, kad žvalgybos informacijos apie grėsmes teikėjų parūpinimas arba paskyrimas būtų užbaigiamas prieš pradedant testavimo etapą.

10. Prieš pradėdama testavimo etapą, kontrolės grupė konsultuojasi su testavimo vadovais dėl TLPT rizikos vertinimo ir rizikos valdymo priemonių. Kontrolės grupė peržiūri rizikos vertinimą arba rizikos valdymo priemones, jei TLPT institucija mano, kad jomis nepakankamai atsižvelgiama į TLPT riziką.

11. Kontrolės grupė įvertina, ar žvalgybos informacijos apie grėsmes teikėjai ir testuotojai, kuriuos svarstoma įtraukti į TLPT, atitinka Reglamento (ES) 2022/2554 27 straipsnyje ir šio reglamento 7 straipsnio 1 dalyje nustatytus reikalavimus, ir dokumentuoja to vertinimo rezultatus. Kontrolės grupė, remdamasi tuo vertinimu ir savo rizikos valdymo praktika, atrenka žvalgybos informacijos apie grėsmes teikėjus. Prieš sudarydama sutartis su atrinktais žvalgybos informacijos apie grėsmes teikėjais ir išorės testuotojais, kontrolės grupė testavimo vadovams pateikia įrodymus, kad tie žvalgybos informacijos apie grėsmes teikėjai ir testuotojai atitinka Reglamento (ES) 2022/2554 27 straipsnyje ir šio reglamento 7 straipsnio 1 dalyje nustatytus reikalavimus. Kontrolės grupė nepradeda sudaryti sutarčių su atrinktais žvalgybos informacijos apie grėsmes teikėjais ir išorės testuotojais, jei TLPT institucija mano, kad atrinkti žvalgybos informacijos apie grėsmes teikėjai ir išorės testuotojai neatitinka Reglamento (ES) 2022/2554 27 straipsnyje arba šio reglamento 7 straipsnio 1 dalyje nustatytų reikalavimų arba papildomų reikalavimų, kylančių iš Sąjungos teisę atitinkančių nacionalinių saugumo teisės aktų, jei finansų sektoriaus subjektas nesilaiko šio reglamento 7 straipsnio 2 dalies pirmos pastraipos arba jei netenkinamos šio reglamento 7 straipsnio 2 dalies antroje pastraipoje nurodytos aplinkybės.

12. Jeigu aprėpties aprašymas yra išsamus ir juo užtikrinamas tinkamas ir veiksmingas TLPT, TLPT institucija patvirtina tą aprašymą ir apie tai informuoja kontrolės grupės vadovą.

10 straipsnis

Testavimo etapas. Žvalgybos informacija apie grėsmes

1. TLPT institucijai patvirtinus aprėpties aprašymą, žvalgybos informacijos apie grėsmes teikėjas išanalizuoja finansų sektoriaus subjektui aktualią bendro pobūdžio ir konkretaus sektoriaus žvalgybos informaciją apie grėsmes. Jeigu TLPT institucija pateikia valstybės narės finansų sektoriaus bendrą grėsmių panoramą, žvalgybos informacijos apie grėsmes teikėjas gali naudoti tą panoramą kaip nacionalinės grėsmių panoramos atskaitos tašką. Žvalgybos informacijos apie grėsmes teikėjas nustato kibernetines grėsmes ir esamus arba galimus finansų sektoriaus subjekto pažeidžiamumus. Be to, žvalgybos informacijos apie grėsmes teikėjas renka ir analizuoja konkrečią, praktiškai pritaikomą ir kontekstinę tikslinę bei žvalgybos informaciją apie grėsmes, susijusias su finansų sektoriaus subjektu, be kita ko, konsultuodamasis su kontrolės grupe ir testavimo vadovais.

2. Žvalgybos informacijos apie grėsmes teikėjas kontrolės grupei, testuotojams ir testavimo vadovams pristato atitinkamas grėsmes ir tikslinę žvalgybos informaciją apie grėsmes ir pasiūlo reikalingus scenarijus. Siūlomi scenarijai skiriasi atsižvelgiant į nustatytus grėsmę keliančius subjektus ir susijusią taktiką, metodus bei procedūras ir kuriami kiekvienai ypatingos svarbos ar svarbiai funkcijai, kuriai taikomas TLPT.

3. Kontrolės grupės vadovas pasirenka bent tris TLPT vykdymo scenarijus, remdamasis visais šiais elementais:

a) žvalgybos informacijos apie grėsmes teikėjo rekomendacija ir kiekvieno grėsmėmis grindžiamo scenarijaus pobūdžiu;

b) testavimo vadovų pateikta informacija;

c) siūlomų vykdymo scenarijų įgyvendinamumu, remiantis testuotojų ekspertiniu vertinimu;

d) finansų sektoriaus subjekto dydžiu, sudėtingumu ir bendru rizikos profiliu, taip pat jo paslaugų, veiklos ir operacijų pobūdžiu, mastu ir sudėtingumu.

4. Ne daugiau kaip vienas iš pasirinktų scenarijų gali būti negrindžiamas grėsmėmis ir gali būti paremtas ateities perspektyvomis grindžiama ir galimai fiktyvia grėsme, turinčia didelę prognozuojamąją, prevencinę, oportunistinę ar perspektyvinę reikšmę, atsižvelgiant į numatomus finansų sektoriaus subjekto grėsmių panoramos pokyčius.

Atliekant bendrą TLPT, nedarant poveikio scenarijams, kurie yra tiesiogiai susiję su testavime dalyvaujančių finansų sektoriaus subjektų ypatingos svarbos arba svarbiomis funkcijomis, bent vienas scenarijus turi būti susijęs su atitinkamomis IRT paslaugas teikiančios trečiosios šalies pagrindinėmis IRT sistemomis, procesais ir technologijomis, kuriomis palaikomos į aprėptį įtrauktų finansų sektoriaus subjektų ypatingos svarbos arba svarbios funkcijos.

Atliekant jungtinį TLPT, kurio metu dalyvauja grupės vidaus IRT paslaugų teikėjas, nedarant poveikio scenarijams, kurie yra tiesiogiai susiję su testavime dalyvaujančių finansų sektoriaus subjektų ypatingos svarbos arba svarbiomis funkcijomis, bent vienas scenarijus turi būti susijęs su atitinkamomis grupės vidaus IRT paslaugų teikėjo IRT sistemomis, procesais ir technologijomis, kuriomis palaikomos į aprėptį įtrauktų finansų sektoriaus subjektų ypatingos svarbos arba svarbios funkcijos.

5. Žvalgybos informacijos apie grėsmes teikėjas kontrolės grupei pateikia tikslinės žvalgybos informacijos apie grėsmes ataskaitą, įskaitant pagal 3 ir 4 dalis parinktus scenarijus. Žvalgybos informacijos apie grėsmes ataskaitoje pateikiama III priede nurodyta informacija.

6. Kontrolės grupė pateikia tikslinės žvalgybos informacijos apie grėsmes ataskaitą testavimo vadovui patvirtinti. Jeigu tikslinės žvalgybos informacijos apie grėsmes ataskaita yra išsami ir ja užtikrinamas veiksmingas TLPT, TLPT institucija patvirtina tą tikslinės žvalgybos informacijos apie grėsmes ataskaitą ir apie tai informuoja kontrolės grupės vadovą.

11 straipsnis

Testavimo etapas. Raudonosios komandos testavimas

1. TLPT institucijai patvirtinus tikslinės žvalgybos informacijos apie grėsmes ataskaitą, testuotojai parengia raudonosios komandos testavimo planą, kuriame pateikiama IV priede nurodyta informacija. Kaip pagrindą išpuolių scenarijams parengti testuotojai naudoja aprėpties aprašymą ir tikslinės žvalgybos informacijos apie grėsmes ataskaitą.

2. Rengdami raudonosios komandos testavimo planą testuotojai konsultuojasi su kontrolės grupe, žvalgybos informacijos apie grėsmes teikėju ir testavimo vadovais, be kita ko, dėl komunikacijos, procedūrų ir projekto valdymo tvarkos, pasiruošimo ir naudojimo scenarijų, susijusių su pagalbinių paslaugų aktyvavimu, ir susitarimų dėl ataskaitų teikimo su kontrolės grupe ir testavimo vadovais.

3. Jei raudonosios komandos testavimo planas yra išsamus ir juo užtikrinamas veiksmingas TLPT, kontrolės grupė ir TLPT institucija raudonosios komandos testavimo planą patvirtina, o TLPT institucija apie tai informuoja kontrolės grupės vadovą.

4. Pagal 3 dalį patvirtinus raudonosios komandos testavimo planą, testuotojai atlieka TLPT aktyviojo raudonosios komandos testavimo etapo metu.

5. Aktyviojo raudonosios komandos testavimo etapo trukmė turi būti proporcinga TLPT aprėpčiai, finansų sektoriaus subjektų ir IRT paslaugas teikiančios trečiosios šalies arba grupės vidaus IRT paslaugų teikėjų, dalyvaujančių TLPT, mastui, veiklai, sudėtingumui ir skaičiui ir bet kuriuo atveju ne trumpesnė kaip 12 savaičių. Išpuolių scenarijai gali būti vykdomi paeiliui arba tuo pačiu metu. Kontrolės grupė, žvalgybos informacijos apie grėsmes teikėjas, testuotojai ir testavimo vadovai susitaria dėl aktyviojo raudonosios komandos testavimo etapo pabaigos.

6. Jeigu užtikrinamas raudonosios komandos testavimo plano išsamumas ir sudaromos sąlygos atlikti veiksmingą TLPT, kontrolės grupės vadovas ir testavimo vadovai patvirtina visus raudonosios komandos testavimo plano pakeitimus, įskaitant pakeitimus, susijusius su tvarkaraščiu, aprėptimi, konkrečiomis sistemomis ar grėsmėmis.

7. Per visą aktyviojo raudonosios komandos testavimo etapą testuotojai bent kartą per savaitę kontrolės grupei ir testavimo vadovams praneša apie padarytą TLPT pažangą, o žvalgybos informacijos apie grėsmes teikėjas kontrolės grupės prašymu teikia konsultacijas ir papildomą žvalgybos informaciją apie grėsmes.

8. Kontrolės grupė laiku suteikia pagal raudonosios komandos testavimo planą parengtas pagalbines paslaugas. Pagalbines paslaugas galima pridėti arba pritaikyti kontrolės grupei ir testavimo vadovams pritarus.

9. Jei bet kuris finansų sektoriaus subjekto, jam IRT paslaugas teikiančių trečiųjų šalių arba, kai aktualu, grupės vidaus IRT paslaugų teikėjo darbuotojas nustato, kad vykdomas testavimas, kontrolės grupė, pasikonsultavusi su testuotojais ir nedarydama poveikio 10 daliai, pasiūlo ir pateikia priemones, kurias pritaikius būtų galima tęsti TLPT, kartu užtikrinant jo slaptumą testavimo vadovams, kad jį būtų galima laikyti galiojančiu.

10. Išimtinėmis aplinkybėmis, dėl kurių kyla poveikio duomenims, žalos turtui ir paties finansų sektoriaus subjekto, jam IRT paslaugas teikiančių trečiųjų šalių ar grupės vidaus IRT paslaugų teikėjų ypatingos svarbos ar svarbių funkcijų, paslaugų ar operacijų sutrikdymo arba jo partnerių ar finansų sektoriaus veiklos sutrikdymo rizika, kontrolės grupės vadovas gali sustabdyti TLPT arba kraštutiniu atveju, kai TLPT kitaip tęsti nebeįmanoma ir jei gaunamas išankstinis TLPT institucijos patvirtinimas, toliau atlikti TLPT vykdant ribotus purpurinės komandos veiksmus. Ribotų purpurinės komandos veiksmų trukmė skaičiuojama nustatant minimalią aktyviojo raudonosios komandos testavimo etapo 12 savaičių trukmę, kaip nurodyta 5 dalyje.

12 straipsnis

Užbaigimo etapas

1. Pasibaigus aktyviojo raudonosios komandos testavimo etapui, kontrolės grupės vadovas informuoja mėlynąją komandą, kad buvo vykdomas TLPT.

2. Per keturias savaites nuo aktyviojo raudonosios komandos testavimo etapo pabaigos testuotojai kontrolės grupei pateikia raudonosios komandos testavimo ataskaitą, kurioje pateikiama V priede nurodyta informacija.

3. Kontrolės grupė nepagrįstai nedelsdama raudonosios komandos testavimo ataskaitą pateikia mėlynajai komandai ir testavimo vadovams.

Testavimo vadovų prašymu pirmoje pastraipoje nurodytoje ataskaitoje neteikiama neskelbtina informacija.

4. Gavusi raudonosios komandos testavimo ataskaitą ir ne vėliau kaip per dešimt savaičių nuo aktyviojo raudonosios komandos testavimo etapo pabaigos mėlynoji komanda kontrolės grupei pateikia mėlynosios komandos testavimo ataskaitą, kurioje pateikiama VI priede nurodyta informacija. Kontrolės grupė nepagrįstai nedelsdama mėlynosios komandos testavimo ataskaitą pateikia testuotojams ir testavimo vadovams.

Testavimo vadovų prašymu pirmoje pastraipoje nurodytoje ataskaitoje neteikiama neskelbtina informacija.

5. Ne vėliau kaip per dešimt savaičių nuo aktyviojo raudonosios komandos testavimo etapo pabaigos mėlynoji komanda ir testuotojai pakartoja TLPT metu atliktus puolamuosius ir gynybinius veiksmus. Kontrolės grupė taip pat atlieka purpurinės komandos veiksmus, susijusius su mėlynosios komandos ir testuotojų bendrai nurodytais klausimais, remdamasi testavimo metu nustatytais pažeidžiamumais ir, kai aktualu, problemomis, kurių nebuvo galima patikrinti aktyviojo raudonosios komandos testavimo etapo metu.

6. Užbaigus pakartojimo ir purpurinės komandos veiksmus, kontrolės grupė, mėlynoji komanda, testuotojai ir žvalgybos informacijos apie grėsmes teikėjai teikia vieni kitiems grįžtamąją informaciją apie TLPT procesą. Grįžtamąją informaciją gali pateikti ir testavimo vadovai.

7. TLPT institucijai pranešus kontrolės grupės vadovui, kad ji įvertino, jog mėlynosios komandos ir raudonosios komandos testavimo ataskaitose buvo pateikta V ir VI prieduose nurodyta informacija, finansų sektoriaus subjektas per aštuonias savaites TLPT institucijai pateikia ataskaitą, kurioje apibendrina atitinkamus TLPT rezultatus, kaip nurodyta Reglamento (ES) 2022/2554 26 straipsnio 6 dalyje, ir kurioje išdėsto VII priede nustatytus elementus patvirtinti.

TLPT institucijos prašymu pirmoje pastraipoje nurodytoje ataskaitoje neteikiama neskelbtina informacija.

13 straipsnis

Koregavimo planas

1. Per aštuonias savaites nuo šio reglamento 12 straipsnio 7 dalyje nurodyto pranešimo finansų sektoriaus subjektas TLPT institucijai ir, jeigu tai ne ta pati institucija, finansų sektoriaus subjekto kompetentingai institucijai pateikia Reglamento (ES) 2022/2554 26 straipsnio 6 dalyje nurodytus koregavimo planus ir dokumentus.

2. 1 dalyje nurodytame koregavimo plane dėl kiekvieno atliekant TLPT nustatyto fakto pateikiama ši informacija:

a) nustatytų trūkumų aprašymas;

b) siūlomų koregavimo priemonių, jų prioritetų nustatymo ir numatomo užbaigimo aprašymas, įskaitant, kai aktualu, priemones, kuriomis būtų galima pagerinti nustatymo, apsaugos, aptikimo ir reagavimo pajėgumus;

c) pagrindinių priežasčių analizė;

d) finansų sektoriaus subjekto darbuotojai arba asmenys, atsakingi už siūlomų koregavimo priemonių ar patobulinimų įgyvendinimą;

e) rizika, susijusi su b punkte nurodytų priemonių neįgyvendinimu, ir, kai aktualu, rizika, susijusi su tokių priemonių įgyvendinimu.

14 straipsnis

Pažymų išdavimas

1. Reglamento (ES) 2022/2554 26 straipsnio 7 dalyje nurodytoje pažymoje turi būti pateikiama VIII priede nustatyta informacija.

2. Jeigu TLPT dalyvavo kelios TLPT institucijos, Reglamento (ES) 2022/2554 26 straipsnio 7 dalyje nurodytą pažymą testuotiems finansų sektoriaus subjektams pateikia pagrindinė TLPT institucija.

15 straipsnis

Naudojimasis vidaus testuotojų paslaugomis

1. Finansų sektoriaus subjektai nustato visas toliau išvardytas naudojimosi vidaus testuotojų paslaugomis priemones:

a) nustato ir įgyvendina vidaus testuotojų valdymo atliekant TLPT politiką;

b) priemones, kuriomis užtikrinama, kad naudojimasis vidaus testuotojų paslaugomis atliekant TLPT neturėtų neigiamo poveikio finansų sektoriaus subjekto bendriesiems gynybiniams ar atsparumo pajėgumams, susijusiems su IRT incidentais, ar neturėtų didelio poveikio išteklių, TLPT metu skiriamų su IRT susijusioms užduotims, prieinamumui;

c) priemones, kuriomis užtikrinama, kad vidaus testuotojai turėtų pakankamai išteklių ir pajėgumų TLPT vykdyti.

a punkte nurodyta politika:

a) apima vidaus testuotojų tinkamumo, kompetencijos, galimų interesų konfliktų vertinimo kriterijus ir nurodo vadovybės pareigas testavimo proceso metu;

b) turi būti dokumentuojama ir periodiškai peržiūrima;

c) užtikrina, kad į vidaus testavimo grupę būtų įtraukiamas testavimo vadovas ir bent du papildomi nariai;

d) reikalauja, kad visi testavimo grupės nariai paskutinius 12 mėnesių būtų finansų sektoriaus subjekto arba grupės vidaus IRT paslaugų teikėjo darbuotojai;

e) apima nuostatas dėl mokymo, kaip atlikti vidaus testuotojų skverbimosi testavimą ir raudonosios komandos testavimą.

2. Jeigu TLPT institucija patvirtina, kad galima naudotis vidaus testuotojų paslaugomis, pagal Reglamento (ES) 2022/2554 27 straipsnio 2 dalies a punktą, TLPT institucija atsižvelgia į šio reglamento 7 straipsnio 1 dalyje nustatytus reikalavimus.

3. Kai finansų sektoriaus subjektas naudojasi vidaus testuotojų paslaugomis, jis užtikrina, kad toks naudojimasis būtų paminėtas toliau nurodytuose dokumentuose:

a) 9 straipsnyje nurodytoje testavimo inicijavimo informacijoje;

b) 12 straipsnio 2 dalyje nurodytoje raudonosios komandos testavimo ataskaitoje;

c) ataskaitoje, kurioje apibendrinami atitinkami TLPT rezultatai, nurodytoje Reglamento (ES) 2022/2554 26 straipsnio 6 dalyje.

4. Grupės vidaus IRT paslaugų teikėjo pasitelkiami testuotojai laikomi finansų sektoriaus subjekto vidaus testuotojais.

16 straipsnis

Bendradarbiavimas ir abipusis pripažinimas

1. Atliekant TLPT, susijusį su finansų sektoriaus subjektu, teikiančiu paslaugas daugiau nei vienoje valstybėje narėje, be kita ko, per filialą, jo TLPT institucija:

a) nustato, kurios priimančiųjų valstybių narių TLPT institucijos dalyvaus atliekant TLPT, atsižvelgiant į tai, ar priimančiosiose valstybėse narėse vykdoma viena ar daugiau ypatingos svarbos ar svarbių funkcijų arba jomis dalijamasi;

b) informuoja pagal a punktą nustatytas TLPT institucijas apie sprendimą atlikti finansų sektoriaus subjekto TLPT;

c) jeigu TLPT institucijos nesusitaria kitaip, TLPT vadovauja finansų sektoriaus subjekto TLPT institucija.

Per 20 darbo dienų nuo informacijos apie būsimą TLPT gavimo dienos priimančiųjų valstybių narių TLPT institucijos gali pareikšti norą stebėti TLPT stebėtojų teisėmis arba paskirti testavimo vadovą, dalyvausiantį TLPT. Pagrindinė TLPT institucija visoms stebėtojų teisėmis dalyvaujančioms TLPT institucijoms pateikia aprėpties aprašymą, apibendrinamąją testavimo ataskaitą, koregavimo planą ir pažymą.

Pagrindinė TLPT institucija viso testavimo metu koordinuoja visas dalyvaujančias TLPT institucijas ir priima visus sprendimus, kurių reikia siekiant tinkamai ir veiksmingai atlikti TLPT. Pagrindinė TLPT institucija gali nustatyti didžiausią dalyvaujančių TLPT institucijų skaičių, jei priešingu atveju kiltų pavojus veiksmingam TLPT.

2. Jeigu finansų sektoriaus subjektas naudojasi to paties grupės vidaus IRT paslaugų teikėjo paslaugomis kaip ir kitose valstybėse narėse įsisteigę finansų sektoriaus subjektai arba priklauso grupei ir naudoja bendras IRT sistemas su kitose valstybėse narėse įsisteigusiais tos pačios grupės finansų sektoriaus subjektais, finansų sektoriaus subjekto TLPT institucija susisiekia su kitų finansų sektoriaus subjektų, kurie grupėje naudojasi to paties grupės vidaus IRT paslaugų teikėjo paslaugomis arba dalijasi IRT sistemomis, TLPT institucijomis ir kartu su jomis įvertina, ar būtų įmanoma ir tinkama atlikti jungtinį šių subjektų TLPT. Pirmenybė teikiama jungtiniam TLPT, o ne atskiriems TLPT, kai dėl to galima sumažinti finansų sektoriaus subjektų ir TLPT institucijų išlaidas ir naudoti mažiau išteklių, su sąlyga, kad nebus daromas neigiamas poveikis testavimo patikimumui ir efektyvumui.

3. Jei atliekamas jungtinis TLPT:

a) finansų sektoriaus subjektų TLPT institucijos, atsižvelgdamos į grupės struktūrą ir testavimo efektyvumą, susitaria, kurį finansų sektoriaus subjektą reikia paskirti atlikti TLPT;

b) TLPT vadovauja pagal a punktą paskirto finansų sektoriaus subjekto TLPT institucija, išskyrus atvejus, kai jungtiniame TLPT dalyvaujančių finansų sektoriaus subjektų TLPT institucijos susitaria kitaip;

c) finansų sektoriaus subjektų, kurie nėra vadovauti jungtiniam TLPT paskirtas finansų sektoriaus subjektas, TLPT institucijos gali pareikšti norą stebėtojų teisėmis stebėti TLPT arba paskirti atliekant tą TLPT dalyvausiantį testavimo vadovą.

Pagrindinė TLPT institucija koordinuoja visų jungtiniame TLPT dalyvaujančių TLPT institucijų veiksmus ir priima visus sprendimus, kurių reikia siekiant, kad jungtinis TLPT būtų vykdomas patikimai ir veiksmingai.

4. Jeigu finansų sektoriaus subjektas ketina vykdyti bendrą TLPT, kaip nurodyta Reglamento (ES) 2022/2554 26 straipsnio 4 dalyje, ir galbūt įtraukti kitose valstybėse narėse įsisteigusius finansų sektoriaus subjektus, jo TLPT institucija susisiekia su kitų finansų sektoriaus subjektų TLPT institucijomis ir kartu su jomis įvertina bendro tų subjektų TLPT įgyvendinamumą ir tinkamumą pagal Reglamento (ES) 2022/2554 26 straipsnio 4 dalį.

5. Jeigu atliekamas bendras TLPT, kaip nurodyta Reglamento (ES) 2022/2554 26 straipsnio 4 dalyje:

a) finansų sektoriaus subjektų TLPT institucijos susitaria, kuris finansų sektoriaus subjektas bus paskirtas vykdyti bendrą TLPT, atsižvelgiant į finansų sektoriaus subjektams teikiamas trečiųjų šalių IRT paslaugas ir testo efektyvumą;

b) TLPT vadovauja pagal a punktą paskirto finansų sektoriaus subjekto TLPT institucija, išskyrus atvejus, kai bendrame TLPT dalyvaujančių finansų sektoriaus subjektų TLPT institucijos susitaria kitaip;

c) finansų sektoriaus subjektų, kurie nėra vadovauti bendram TLPT paskirtas finansų sektoriaus subjektas, TLPT institucijos gali pareikšti norą stebėtojų teisėmis stebėti TLPT arba paskirti atliekant tą TLPT dalyvausiantį testavimo vadovą.

Pagrindinė TLPT institucija koordinuoja visų bendrame TLPT dalyvaujančių TLPT institucijų veiksmus ir priima visus sprendimus, kurių reikia siekiant, kad bendras TLPT būtų vykdomas patikimai ir veiksmingai.

6. Jeigu finansų sektoriaus subjekto, kuriam būtina atlikti TLPT, TLPT institucija yra ne ta pati, kaip jo kompetentinga institucija, nurodyta Reglamento (ES) 2022/2554 46 straipsnyje, tos institucijos TLPT arba savo pareigų pagal tą reglamentą vykdymo tikslais dalijasi visa svarbia informacija apie visus su TLPT susijusius klausimus.

17 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2025 m. vasario 13 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

Projekto aprašymo turinys (9 straipsnio 2 dalies a punktas)

Informacinis įrašas	Pateiktina informacija
Už projekto planą atsakingas asmuo, t. y. kontrolės grupės vadovas	Vardas ir pavardė Kontaktinė informacija
Testuotojai	☐ vidaus ☐ išorės ☐ ir vidaus, ir išorės
Pagal 9 straipsnio 2 dalies d punktą ir 4 dalies a punktą parinkti ryšių kanalai, įskaitant: a) naudotiną e. pašto šifravimą; b) naudotinas internetines duomenų saugyklas; c) naudotinas tikralaikių pokalbių priemones.	
TLPT kodinis pavadinimas	
Ypatingos svarbos arba svarbios funkcijos, kurias finansų sektoriaus subjektas vykdo kitose valstybėse narėse, jei tokių yra	1. kitoje valstybėje narėje vykdomų ypatingos svarbos arba svarbių funkcijų sąrašas 2. valstybė (-ės) narė (-ės), kurioje (-iose) vykdoma kiekviena ypatingos svarbos arba svarbi funkcija
Ypatingos svarbos arba svarbios funkcijos, kurias palaiko IRT paslaugas teikiančios trečiosios šalys, jei tokių yra	3. ypatingos svarbos arba svarbių funkcijų, kurias palaiko IRT paslaugas teikiančios trečiosios šalys, sąrašas 4. su kiekviena funkcija susijusias IRT paslaugas teikiančios trečiosios šalies nustatymo duomenys
Numatomi užbaigimo terminai	
(1) Parengiamojo etapo, pagal 9 straipsnį	mmmm-mm-dd
(2) Testavimo etapo, pagal 10 ir 11 straipsnius	mmmm-mm-dd
(3) Užbaigimo etapo, pagal 12 straipsnį	mmmm-mm-dd
(4) Koregavimo plano, pagal 13 straipsnį	mmmm-mm-dd

II PRIEDAS

Aprėpties aprašymo turinys (9 straipsnio 6 dalis)

1. Aprėpties aprašyme pateikiamas visų finansų sektoriaus subjekto nustatytų ypatingos svarbos arba svarbių funkcijų sąrašas.

2. Pateikiama toliau nurodyta su kiekviena nustatyta ypatingos svarbos arba svarbia funkcija susijusi informacija:
   a) jeigu ypatingos svarbos arba svarbiai funkcijai netaikomas TLPT, pateikiamas paaiškinimas, kodėl jis netaikomas;
   b) jeigu ypatingos svarbos arba svarbiai funkcijai TLPT taikomas:
      i) pateikiamas paaiškinimas, kodėl tai funkcijai taikomas TLPT;
      ii) nurodoma (-os) IRT sistema (-os), kuria (-iomis) palaikoma ta ypatingos svarbos arba svarbi funkcija;
      iii) kiekvienos nustatytos IRT sistemos informacija:
         1. ar tą sistemą teikia išorės paslaugų teikėjas ir, jei taip, IRT paslaugas teikiančios trečiosios šalies pavadinimas;
         2. jurisdikcijos, kuriose naudojama IRT sistema;
         3. preliminarios (-ių) grėsmės (-ių) aukšto lygio aprašymas, kuriame nurodoma, kuris konfidencialumo, vientisumo, autentiškumo ar prieinamumo saugumo aspektas yra testuojamas nustatant kiekvieną grėsmę.

III PRIEDAS

Tikslinės žvalgybos informacijos apie grėsmes ataskaitos turinys (10 straipsnio 5 dalis)

Tikslinės žvalgybos informacijos apie grėsmes ataskaitoje pateikiama informacija apie visus toliau išvardytus aspektus:

1. bendra žvalgybos tyrimų apimtis, įskaitant bent šiuos elementus:
   a) testuojamas ypatingos svarbos arba svarbias funkcijas;
   b) geografinę vietą;
   c) vartojamą oficialiąją ES kalbą;
   d) atitinkamas IRT paslaugas teikiančias trečiąsias šalis;
   e) laikotarpį, per kurį renkami tyrimo duomenys;
2. bendras įvertinimas, kokios konkrečios žvalgybos informacijos apie finansų sektoriaus subjektą galima rasti, įskaitant:
   a) darbuotojų naudotojų vardus ir slaptažodžius;
   b) panašius domenus, kuriuos galima klaidingai palaikyti oficialiais finansų sektoriaus subjekto domenais;
   c) techninio iššvalgymo informaciją: pažeidžiamą arba tinkamą išnaudoti programinę įrangą, sistemas ir technologijas;
   d) darbuotojų internete skelbiamą informaciją, susijusią su finansų sektoriaus subjektu, kuri gali būti naudojama išpuolio tikslais;
   e) informaciją, kurią galima parduoti „juodajame tinkle“;
   f) bet kokią kitą svarbią informaciją, prieinamą internete arba viešuosiuose tinkluose;
   g) kai aktualu, fizinio poveikio darymo informaciją, įskaitant patekimo į finansų sektoriaus subjekto patalpas būdus;
3. žvalgybos informacijos apie grėsmes analizė atsižvelgiant į bendrą grėsmių panoramą ir konkrečią finansų sektoriaus subjekto padėtį, įskaitant bent šiuos aspektus:
   a) geopolitinę aplinką;
   b) ekonominę aplinką;
   c) technologines tendencijas ir bet kokias kitas tendencijas, susijusias su finansinių paslaugų sektoriaus veikla;
4. piktavalių subjektų (konkretaus asmens / grupės ar bendro pobūdžio kategorijos), kurie gali stengtis daryti poveikį finansų sektoriaus subjektams, grėsmių profiliai, įskaitant finansų sektoriaus subjektus, kuriems piktavaliai subjektai yra labiausiai linkę kelti pavojų arba stengtis daryti poveikį, sistemos, galimi motyvai, ketinimai ir galimas užpuolikų *modus operandi*;
5. grėsmių scenarijai: bent trys ištisiniai grėsmių scenarijai, susiję su pagal 4 punktą nustatytais grėsmių profiliais, kurių grėsmių sunkumo įverčiai yra didžiausi. Grėsmių scenarijuose aprašomas ištisinis išpuolio kelias ir pateikiami bent:
   a) vienas scenarijus, apimantis, be kita ko, paslaugos prieinamumui sukeltą pavojų;
   b) vienas scenarijus, apimantis, be kita ko, duomenų vientisumui sukeltą pavojų;
   c) vienas scenarijus, apimantis, be kita ko, informacijos konfidencialumui sukeltą pavojų;
6. jei aktualu, 10 straipsnio 4 dalyje nurodyto grėsmėmis negrindžiamo scenarijaus aprašymas.

IV PRIEDAS

Raudonosios komandos testavimo plano turinys (11 straipsnio 1 dalis)

Raudonosios komandos testavimo plane pateikiama visa toliau nurodyta informacija:

a) ryšių kanalai ir procedūros;

b) taktika, metodai ir procedūros, kuriuos leidžiama ir neleidžiama naudoti išpuolio metu, įskaitant etines socialinės inžinerijos ribas;

c) rizikos valdymo priemonės, kurių turi laikytis testuotojai;

d) kiekvieno scenarijaus aprašymas, įskaitant:

   i) imituojamą grėsmę keliantį subjektą;

   ii) jo ketinimus, motyvaciją ir tikslus;

   iii) funkciją (-as) ir pagalbinę IRT sistemą ar sistemas, kurioms stengiamasi daryti poveikį;

   iv) konfidencialumo, vientisumo, prieinamumo ir autentiškumo aspektus, kuriems stengiamasi daryti poveikį;

   v) sukeltas grėsmes;

e) išsamus kiekvieno numatomo išpuolio kelio aprašymas, įskaitant būtinas sąlygas ir galimas pagalbines paslaugas, kurias turi teikti kontrolės grupė, įskaitant tokių paslaugų suteikimo ir galimo naudojimosi jomis terminus;

f) raudonosios komandos veiksmų planas, įskaitant suplanuotus kiekvieno scenarijaus įgyvendinimo laikotarpius, bent pagal tris etapus, kuriuos testuotojas įgyvendina per visą testavimo procesą: atitinkamai patekimo į finansų sektoriaus subjektų IRT sistemas, „judėjimo“ IRT sistemose, veiksmų, susijusių su tikslais, įgyvendinimo ir galiausiai pasitraukimo iš IRT sistemų (patekimo, veikimo ir pasitraukimo etapai);

g) finansų sektoriaus subjektų infrastruktūros ypatumai, į kuriuos reikia atsižvelgti atliekant testavimą;

h) jei yra, papildoma informacija ar kiti ištekliai, kurių reikia testuotojams įgyvendinant scenarijus.

V PRIEDAS

Raudonosios komandos testavimo ataskaitos turinys (12 straipsnio 2 dalis)

Raudonosios komandos testavimo ataskaitoje pateikiama bent visa toliau nurodyta informacija:

a) informacija apie įvykdytą išpuolį, įskaitant:

   i) raudonosios komandos testavimo plane nurodytas ypatingos svarbos arba svarbias funkcijas ir nustatytas IRT sistemas, procesus ir technologijas, kuriais palaikoma ypatingos svarbos arba svarbi funkcija ir kuriems buvo siekiama padaryti poveikį;

   ii) kiekvieno scenarijaus santrauką;

   iii) sukeltas ir nesukeltas grėsmes;

   iv) sėkmingai ir nesėkmingai įvykdytų išpuolių kelius;

   v) sėkmingai ir nesėkmingai panaudotą taktiką, metodus ir procedūras;

   vi) nukrypimus nuo raudonosios komandos testavimo plano, jei jų buvo;

   vii) suteiktas pagalbines paslaugas, jei jų buvo;

b) visi testuotojams žinomi veiksmai, kuriuos atliko mėlynoji komanda, siekdama atkurti išpuolį ir sušvelninti jo padarinius;

c) nustatyti pažeidžiamumai ir kiti nustatyti faktai, įskaitant:

   i) pažeidžiamumų ir kitų nustatytų faktų, įskaitant jų svarbumą, aprašymą;

   ii) pavykusių išpuolių pagrindinių priežasčių analizę;

   iii) rekomendacijas dėl koregavimo, įskaitant koregavimo veiksmų prioritetų nustatymą.

VI PRIEDAS

Mėlynosios komandos testavimo ataskaitos turinys (12 straipsnio 4 dalis)

Mėlynosios komandos testavimo ataskaitoje pateikiama bent visa toliau nurodyta informacija:

1. kiekvieno išpuolio etapo, testuotojų aprašyto raudonosios komandos testavimo ataskaitoje, informacija:
   a) aptiktų išpuolio veiksmų sąrašas;
   b) tų aptiktų veiksmų registracijos įrašai;
2. testuotojų nustatytų faktų ir rekomendacijų vertinimas;
3. mėlynosios komandos surinkti įrodymai, kad testuotojai įvykdė išpuolį;
4. mėlynosios komandos atlikta testuotojų pavykusių išpuolių pagrindinių priežasčių analizė;
5. įgytos patirties ir nustatytų tobulinimo galimybių sąrašas;
6. klausimų, kuriuos reikės spręsti atliekant purpurinės komandos veiksmus, sąrašas.

VII PRIEDAS

Išsami informacija apie ataskaitą, kurioje apibendrinami atitinkami TLPT rezultatai, nurodytą Reglamento (ES) 2022/2554 26 straipsnio 6 dalyje

Apibendrinamojoje testavimo ataskaitoje pateikiama bent visa toliau nurodyta informacija:

a) dalyvavusios šalys;

b) projekto planas;

c) patvirtinta aprėptis, įskaitant ypatingos svarbos ar svarbių funkcijų ir nustatytų IRT sistemų, procesų ir technologijų, palaikančių ypatingos svarbos ar svarbias funkcijas, kurioms buvo taikomas TLPT, įtraukimo ar neįtraukimo pagrindimas;

d) pasirinkti scenarijai ir bet kokie reikšmingi nukrypimai nuo tikslinės žvalgybos informacijos apie grėsmes ataskaitos;

e) įvykdytų išpuolių keliai ir naudota taktika, metodai ir procedūros;

f) sukeltos ir nesukeltos grėsmės;

g) nukrypimai nuo raudonosios komandos testavimo plano, jei jų buvo;

h) mėlynosios komandos aptikimai, jei jų buvo;

i) purpurinės komandos veiksmai testavimo etape, jeigu jie buvo vykdomi, ir kokios buvo susijusios sąlygos;

j) panaudotos pagalbinės paslaugos, jei jų buvo;

k) rizikos valdymo priemonės, kurių buvo imtasi;

l) nustatyti pažeidžiamumai ir kiti nustatyti faktai, įskaitant jų svarbumą;

m) pavykusių išpuolių pagrindinių priežasčių analizė;

n) aukšto lygio koregavimo planas, kuriame susiejami pažeidžiamumai ir kiti nustatyti faktai, jų pagrindinės priežastys ir žalos koregavimo veiksmų prioritetai;

o) patirtis, įgyta gavus grįžtamąją informaciją.

VIII PRIEDAS

Išsami informacija apie Reglamento (ES) 2022/2554 26 straipsnio 7 dalyje nurodytą TLPT pažymą

Pažymoje pateikiama bent visa toliau nurodyta informacija:

a) informacija apie atliktą TLPT:
   i) TLPT pradžios ir pabaigos datos;
   ii) ypatingos svarbos arba svarbios funkcijos, kurios buvo testuojamos;
   iii) jeigu aktualu, informacija apie ypatingos svarbos arba svarbias funkcijas, kurių TLPT nebuvo atliekamas;
   iv) jeigu aktualu, kiti finansų sektoriaus subjektai, kurie buvo įtraukti į TLPT;
   v) jeigu aktualu, IRT paslaugas teikiančios trečiosios šalys, kurios dalyvavo TLPT;
   vi) informacija apie testuotojus:
      1. ar buvo pasitelkiami vidaus testuotojai;
      2. ar finansų sektoriaus subjektas taikė 5 straipsnio 3 dalies antrą pastraipą;
   vii) aktyviojo raudonosios komandos testavimo etapo trukmė kalendorinėmis dienomis;
b) jeigu atliekant TLPT dalyvavo kelios TLPT institucijos, kitos TLPT institucijos ir jų dalyvavimo mastas;
c) dokumentų, kuriuos TLPT institucija išnagrinėjo rengdama pažymą, sąrašas.