Uradni list
Evropske unije

SL
Serija L

2025/1190

18.6.2025

DELEGIRANA UREDBA KOMISIJE (EU) 2025/1190

z dne 13. februarja 2025

o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo merila, ki se uporabljajo za opredelitev finančnih subjektov, ki morajo izvajati penetracijsko testiranje na podlagi groženj, zahteve in standarde, ki urejajo uporabo notranjih preizkuševalcev, zahteve v zvezi z obsegom, metodologijo in pristopom testiranja za vsako fazo testiranja, rezultate, zaključno fazo in fazo sanacije ter vrsto sodelovanja nadzornih organov in drugega ustreznega sodelovanja, ki je potrebno za izvedbo penetracijskega testiranja na podlagi analize groženj in njegovo lažje vzajemno priznavanje

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 ([1]) ter zlasti člena (26)11, četrti pododstavek, Uredbe,

ob upoštevanju naslednjega:

(1) Ta uredba je bila pripravljena v skladu z okvirom TIBER-EU ter odraža metodologijo, postopek in strukturo penetracijskega testiranja na podlagi groženj (v nadaljnjem besedilu: TLPT), kot je opisano v TIBER-EU. Finančni subjekti, ki morajo izvajati TLPT, se lahko sklicujejo na okvir TIBER-EU ali eno od njegovih nacionalnih izvedb in ga uporabljajo, če je ta okvir ali izvedba v skladu z zahtevami iz členov 26 in 27 Uredbe (EU) 2022/2554 in te uredbe. Imenovanje enega samega javnega organa v finančnem sektorju, ki je na nacionalni ravni odgovoren za zadeve, povezane s TLPT, v skladu s členom 26(9) Uredbe (EU) 2022/2554, ne bi smelo posegati v pristojnost pristojnih organov, ki so na ravni Unije pooblaščeni za nadzor nekaterih finančnih subjektov v skladu s členom 46 navedene uredbe, kot je na primer Evropska centralna banka za pomembne kreditne institucije, ki se štejejo za pristojne za zadeve, povezane s TLPT. Kadar se le nekatere naloge, povezane s TLPT, prenesejo na drug nacionalni organ v finančnem sektorju v skladu s členom 26(10) Uredbe (EU) 2022/2554, bi moral pristojni organ finančnega subjekta iz člena 46 navedene uredbe ostati pristojni organ za naloge, povezane s TLPT, ki niso bile prenesene.

(2) Glede na zapletenost TLPT in z njim povezana tveganja bi bilo treba njegovo uporabo omejiti na tiste finančne subjekte, za katere je upravičena. Zato bi morali organi, pristojni za vprašanja v zvezi s TLPT (organi za TLPT na ravni Unije ali nacionalni ravni), iz področja uporabe TLPT izključiti tiste finančne subjekte, ki delujejo v osrednjih podsektorjih finančnih storitev, za katere TLPT ni upravičen. To pomeni, da bi lahko bili kreditne institucije, plačilne institucije in institucije za izdajo elektronskega denarja, centralne depotne družbe, centralne nasprotne stranke, mesta trgovanja, zavarovalnice in pozavarovalnice, čeprav izpolnjujejo kvantitativna merila, oproščeni zahteve po TLPT ob upoštevanju celovite ocene njihovega profila tveganja in stopnje zrelosti na področju IKT, vpliva na finančni sektor in s tem povezanih pomislekov glede finančne stabilnosti.

(3) Organi za TLPT bi morali ob upoštevanju celovite ocene profila tveganja in stopnje zrelosti na področju IKT, vpliva na finančni sektor in s tem povezanih pomislekov glede finančne stabilnosti oceniti, ali bi katera koli vrsta finančnega subjekta, ki ni kreditna institucija, plačilna institucija, institucija za izdajo elektronskega denarja, centralna nasprotna stranka, centralna depotna družba, mesto trgovanja, zavarovalnica ali pozavarovalnica, morala izvajati TLPT Ocena, ali taki finančni subjekti izpolnjujejo ta kvalitativna merila, bi morala biti namenjena temu, da se z uporabo medsektorskih in objektivnih kazalnikov opredelijo finančni subjekti, za katere je ustrezno izvajanje TLPT. Hkrati bi morala ocena, ali finančni subjekt izpolnjuje ta kvalitativna merila, omejiti subjekte, ki morajo izvajati TLPT, na tiste,

([1]) UL L 333, 27.12.2022, str. 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

za katere je testiranje upravičeno. Ali finančni subjekt izpolnjuje ta kvalitativna merila, bi bilo treba oceniti tudi glede na razvoj novih trgov in vse večji pomen novih udeležencev na trgu za finančni sektor v prihodnosti, vključno s ponudniki storitev v zvezi s kriptosredstvi, ki imajo dovoljenje v skladu s členom 59 Uredbe (EU) 2023/1114 Evropskega parlamenta in Sveta ([2]).

(4) Finančni subjekti imajo lahko istega ponudnika storitev IKT znotraj skupine ali pripadajo isti skupini in uporabljajo skupne sisteme IKT. V tem primeru je pomembno, da organi za TLPT pri oceni, ali bi finančni subjekt moral izvajati TLPT in ali bi bilo treba TLPT izvajati na ravni subjekta ali skupine (v obliki skupinskega TLPT), upoštevajo strukturo in sistemski značaj ali pomen tega finančnega subjekta za finančni sektor na nacionalni ravni ali ravni Unije.

(5) Da bi se odražal okvir TIBER-EU, mora metodologija testiranja zagotoviti sodelovanje naslednjih glavnih udeležencev: finančnega subjekta z nadzorno ekipo (ki odraža „nadzorno ekipo“ TIBER-EU) in modro ekipo (ki odraža „modro ekipo“ TIBER-EU) ter organa za TLPT v obliki kibernetske ekipe za TLPT (ki odraža „kibernetske ekipe TIBER“ TIBER-EU), ponudnika obveščevalnih podatkov o grožnjah in preizkuševalcev (pri čemer preizkuševalci odražajo „ponudnika rdeče ekipe“ TIBER-EU).

(6) Za zagotovitev, da TLPT izkoristi izkušnje, pridobljene v okviru izvajanja TIBER-EU, in za zmanjšanje tveganj, povezanih z izvajanjem TLPT, bi bilo treba zagotoviti, da se odgovornosti kibernetskih ekip za TLPT, ki bodo vzpostavljene na ravni organov za TLPT, čim bolj ujemajo z odgovornostmi kibernetskih ekip TIBER-EU. Zato bi morale imeti kibernetske ekipe za TLPT vodje testiranja, ki so odgovorni za nadzor posameznih izvedb TLPT ter za načrtovanje in usklajevanje posameznih testov. Kibernetske ekipe za TLPT bi morale delovati kot enotna kontaktna točka za komunikacijo z notranjimi in zunanjimi deležniki v zvezi s testiranjem, za zbiranje in obdelavo povratnih informacij in izkušenj, pridobljenih s predhodno opravljenimi testi, ter za podporo finančnim subjektom, v katerih poteka TLPT.

(7) Da bi se odražala okvirna metodologija TIBER-EU, bi morali imeti vodje testiranja potrebne spretnosti in zmogljivosti za svetovanje in kritičnost do predlogov preizkuševalcev. Izkušnje v okviru TIBER-EU so pokazale, da je koristno, če se za vsak test dodeli ekipa vsaj dveh vodij testiranja. Da bi se odrazilo, da se TLPT uporablja za spodbujanje učnih izkušenj, se zaradi varovanja zaupnosti testov in razen v primeru težav z viri ali s strokovnim znanjem močno priporoča, da organi za TLPT upoštevajo, da vodje testiranja v času trajanja TLPT ne bi smeli izvajati nadzornih dejavnosti v istem finančnem subjektu, v katerem poteka TLPT.

(8) Zaradi skladnosti z okvirom TIBER-EU je pomembno, da organ za TLPT pozorno spremlja vse faze testiranja. Glede na naravo testiranja in z njim povezana tveganja je bistveno, da je organ za TLPT vključen v vsako posamezno fazo testiranja. Zlasti bi se bilo treba posvetovati z organom za TLPT, ki bi moral potrditi tiste ocene ali odločitve finančnih subjektov, ki lahko po eni strani vplivajo na učinkovitost testa, po drugi strani pa na tveganja, povezana s testom. Med temeljnimi koraki, pri katerih je potrebno posebno sodelovanje organa za TLPT, sta potrditev določene temeljne dokumentacije o testiranju ter izbira ponudnikov obveščevalnih podatkov o grožnjah in preizkuševalcev ter ukrepov za obvladovanje tveganj. Sodelovanje organov za TLPT, zlasti pri potrjevanju, ne bi smelo povzročiti prevelikega bremena za te organe, zato bi moralo biti omejeno na dokumentacijo in odločitve, ki neposredno vplivajo na izvajanje TLPT. Organi za TLPT lahko z dejavnim sodelovanjem v vsaki fazi testiranja učinkovito ocenijo skladnost finančnih subjektov z zadevnimi zahtevami, kar bi moralo tem organom omogočiti izdajanje potrdil v skladu s členom 26(7) Uredbe (EU) 2022/2554.

([2]) Uredba (EU) 2023/1114 Evropskega parlamenta in Sveta z dne 31. maja 2023 o trgih kriptosredstev in spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937 (UL L 150, 9.6.2023, str. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Tajnost TLPT je izjemno pomembna za zagotovitev realističnih pogojev testiranja. Zato bi moralo biti testiranje prikrito, za ohranitev zaupnosti TLPT pa bi bilo treba sprejeti previdnostne ukrepe, vključno z izbiro šifer, s katerimi bi tretjim osebam preprečili, da prepoznajo TLPT. Če bi bili zaposleni, ki so odgovorni za varnost finančne skupine, seznanjeni z načrtovanim ali potekajočim TLPT, bi bili verjetno bolj pazljivi in bolj pozorni kot v običajnih delovnih pogojih, zaradi česar bi bil rezultat testiranja drugačen. Zaposlene pri finančnem subjektu, ki niso v nadzorni ekipi, bi bilo zato treba o načrtovanem ali potekajočem TLPT obvestiti le v primeru tehtnih razlogov in s predhodnim soglasjem vodij testiranja, med drugim, da se zagotovi tajnost testiranja, če je kdo izmed članov modre ekipe odkril testiranje.

(10) Kot kažejo izkušnje, pridobljene v okviru TIBER-EU v zvezi z „nadzorno ekipo“, je izbira ustreznega vodje nadzorne ekipe nujna za varno izvajanje TLPT. Vodja nadzorne ekipe mora imeti potrebna pooblastila v finančnem subjektu za usmerjanje vseh vidikov testiranja, ne da bi bila pri tem ogrožena njegova zaupnost. Iz istega razloga morajo biti člani nadzorne ekipe dobro seznanjeni s finančnim subjektom, delovno vlogo in strateškim položajem vodje nadzorne ekipe, imeti morajo zahtevano delovno dobo in dostop do upravnega odbora. Da bi zmanjšali tveganje ogrožanja zaupnosti TLPT, mora biti nadzorna ekipa čim manjša.

(11) Obstajajo inherentni elementi tveganj, povezanih s TLPT, saj se kritične funkcije testirajo v aktivnem produkcijskem okolju, z možnostjo povzročitve incidentov za zavrnitev storitve, nepričakovanega sesutja sistema, poškodb kritičnih aktivnih produkcijskih sistemov ali izgube, spremembe ali razkritja podatkov. Ta tveganja poudarjajo potrebo po zanesljivih ukrepih za obvladovanje tveganj. Za zagotovitev nadzorovanega izvajanja TLPT med celotnim testiranjem je zelo pomembno, da se finančni subjekti na vseh točkah zavedajo posebnih tveganj, ki se pojavljajo pri TLPT, in da se ta tveganja zmanjšajo. V zvezi s tem je lahko brez poseganja v notranje postopke finančnega subjekta ter odgovornost in prenose, ki so že bili predloženi vodji nadzorne ekipe, ustrezno, da je upravljalni organ finančnega subjekta obveščen o ukrepih za obvladovanje tveganj TLPT, v posebnih primerih pa te ukrepe odobri. Da bi lahko zagotavljali učinkovite in visokokvalificirane strokovne storitve ter zmanjšali ta tveganja, je bistveno tudi, da imajo preizkuševalci in ponudniki obveščevalnih podatkov o grožnjah (skupaj ponudniki TLPT) najvišjo raven spretnosti, strokovnega znanja in ustreznih izkušenj na področju obveščevalnih podatkov o grožnjah in TLPT v sektorju finančnih storitev.

(12) Konvencionalni penetracijski testi zagotavljajo podrobno in koristno oceno tehničnih in konfiguracijskih ranljivosti, ki pogosto zadevajo en sam sistem ali ločeno okolje, vendar v nasprotju s testom rdeče ekipe na podlagi obveščevalnih podatkov ne ocenjujejo izčrpnega scenarija ciljno usmerjenega napada na celoten subjekt, vključno s celotnim obsegom njegovih ljudi, postopkov in tehnologij. Med izbirnim postopkom ponudnikov TLPT bi morali finančni subjekti zato zagotoviti, da imajo ti ponudniki potrebne spretnosti za izvajanje testov rdeče ekipe na podlagi obveščevalnih podatkov in ne le penetracijskih testov. Zato je treba določiti celovita merila za preizkuševalce, tako notranje kot zunanje, ter ponudnike obveščevalnih podatkov o grožnjah, ki so vedno zunanji. Kadar ponudniki TLPT pripadajo istemu podjetju, bi bilo treba zaposlene, dodeljene za TLPT, ustrezno ločiti.

(13) V izjemnih okoliščinah se lahko zgodi, da finančni subjekti ne morejo skleniti pogodbe s ponudniki TLPT, ki izpolnjujejo celovita merila. Finančnim subjektom, ki dokažejo nerazpoložljivost takih ponudnikov obveščevalnih podatkov o grožnjah, bi bilo zato treba dovoliti, da najamejo osebe, ki ne izpolnjujejo vseh celovitih meril, pod pogojem, da ustrezno zmanjšajo vsa iz tega izhajajoča dodatna tveganja in da organ za TLPT oceni vsa ta merila.

(14) Kadar je v TLPT vključenih več finančnih subjektov in več organov za TLPT, bi bilo treba določiti vloge vseh strani v postopku TLPT za izvedbo najučinkovitejšega in najvarnejšega testiranja. Za namene skupnega testiranja so potrebne posebne zahteve za opredelitev vloge določenega finančnega subjekta, in sicer da bi moral biti odgovoren za zagotavljanje vse potrebne dokumentacije vodilnemu organu za TLPT in za spremljanje postopka testiranja. Določeni finančni subjekt bi moral biti odgovoren tudi za skupne vidike ocene obvladovanja tveganj. Ne glede na vlogo določenega finančnega subjekta bi morale obveznosti vsakega finančnega subjekta, ki sodeluje v postopku skupnega TLPT, med skupnim testiranjem ostati nespremenjene. Enako načelo bi se moralo uporabljati za skupinski TLPT.

(15) Kot dokazujejo izkušnje z izvajanjem okvira TIBER-EU, je organizacija sestankov s fizično prisotnostjo ali virtualnih sestankov z vsemi zadevnimi deležniki (finančnimi subjekti, organi, preizkuševalci in ponudniki obveščevalnih podatkov o grožnjah) najučinkovitejši način za zagotovitev ustreznega izvajanja testiranja. Sestanki s fizično prisotnostjo in virtualni sestanki bi zato morali potekati v različnih fazah postopka, zlasti v pripravljalni fazi in ob začetku izvajanja TLPT za dokončno določitev njegovega obsega, v fazi testiranja, da se izdela poročilo o obveščevalnih podatkih o grožnjah in načrt testiranja rdeče ekipe ter za tedensko obveščanje, ter v zaključni fazi za ponovitev ukrepov preizkuševalcev in modre ekipe, povezovanje v vijolično ekipo in izmenjavo povratnih informacij o TLPT.

(16) Za zagotovitev nemotenega izvajanja TLPT bi moral organ za TLPT finančnemu subjektu jasno predstaviti svoja pričakovanja v zvezi s testiranjem. V zvezi s tem bi morali vodje testiranja zagotoviti vzpostavitev ustreznega pretoka informacij z nadzorno ekipo znotraj finančnega subjekta in s ponudniki TLPT.

(17) Finančni subjekt bi moral izbrati kritične ali pomembne funkcije, ki bodo vključene v obseg TLPT. Pri izbiri teh funkcij bi se moral finančni subjekt opreti na različna merila glede na pomembnost vsake funkcije za sam finančni subjekt in za finančni sektor na ravni Unije in nacionalni ravni, ne le v gospodarskem smislu, temveč tudi ob upoštevanju simboličnega ali političnega statusa funkcije. Za lažji prehod v fazo zbiranja obveščevalnih podatkov o grožnjah bi morala nadzorna ekipa preizkuševalcem in ponudnikom obveščevalnih podatkov o grožnjah, ki niso vključeni v postopek določanja obsega, zagotoviti podrobne informacije o dogovorjenem določanju obsega.

(18) Da bi preizkuševalcem zagotovili informacije, potrebne za simulacijo resničnega in realističnega napada na aktivne sisteme finančnega subjekta, na katerih temeljijo njegove kritične ali pomembne funkcije, bi moral ponudnik obveščevalnih podatkov o grožnjah zbirati obveščevalne podatke ali informacije, ki zajemajo vsaj dve ključni interesni področji: tarče, tako da opredeli morebitne napadne površine v celotnem finančnem subjektu, in grožnje, tako da opredeli ustrezne akterje groženj in verjetne scenarije groženj. Da se zagotovi, da ponudnik obveščevalnih podatkov o grožnjah upošteva relevantne grožnje za finančni subjekt, bi morali preizkuševalci, nadzorna ekipa in vodje testiranj podati povratne informacije glede osnutka poročila o obveščevalnih podatkih o grožnjah. Ponudnik obveščevalnih podatkov o grožnjah lahko kot izhodišče za nacionalno krajino groženj uporabi splošno krajino groženj, ki jo organ za TLPT zagotovi za finančni sektor države članice, če je na voljo. Na podlagi uporabe okvira TIBER-EU postopek zbiranja obveščevalnih podatkov o grožnjah običajno traja približno štiri tedne.

(19) Da bi preizkuševalci lahko dobili vpogled in nadalje pregledali dokument s specifikacijo obsega in ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah, da bi pripravili načrt testiranja rdeče ekipe, je bistveno, da preizkuševalci pred fazo testiranja rdeče ekipe v okviru TLPT od ponudnika obveščevalnih podatkov o grožnjah prejmejo podrobna pojasnila o ciljno usmerjenem poročilu o obveščevalnih podatkih o grožnjah in analizo možnih scenarijev groženj.

(20) Da bi preizkuševalci lahko izvedli realistično in celovito testiranje, v katerem se izvedejo vse faze napada in dosežejo oznake, bi bilo treba za fazo aktivnega testiranja rdeče ekipe dodeliti dovolj časa. Na podlagi pridobljenih izkušenj v okviru TIBER-EU bi moral dodeljeni čas obsegati najmanj 12 tednov, določiti pa bi ga bilo treba ob upoštevanju števila udeleženih strani, obsega TLPT, virov vključenega finančnega subjekta ali subjektov, morebitnih zunanjih zahtev in razpoložljivosti podpornih informacij, ki jih predloži finančni subjekt.

(21) V fazi aktivnega testiranja rdeče ekipe bi morali preizkuševalci uporabiti vrsto taktik, tehnik in postopkov za ustrezno testiranje aktivnih produkcijskih sistemov finančnega subjekta. Taktike, tehnike in postopki bi morali po potrebi vsebovati izvidništvo (tj. zbiranje čim več informacij o tarči), uporabo kot orožje (tj. analizo informacij o infrastrukturi, objektih in zaposlenih ter pripravo na specifične operacije proti tarči), izvedbo (tj. aktivni začetek obsežne operacije proti tarči), izkoriščanje (tj. kadar želi preizkuševalec ogroziti strežnike in omrežja finančnega subjekta ter izkoristiti njegove zaposlene s socialnim inženiringom), nadzor in premike (tj. poskuse prehoda z ogroženih sistemov na druge ranljive sisteme ali sisteme visoke vrednosti) ter ukrepe proti tarči (tj. pridobitev dodatnega dostopa do ogroženih sistemov in pridobitev dostopa do vnaprej dogovorjenih ciljnih informacij in podatkov, kot je bilo predhodno dogovorjeno v načrtu testiranja rdeče ekipe).

(22) Pri izvajanju TLPT bi morali preizkuševalci upoštevati čas, ki je na voljo za izvedbo napada, vire ter etične in pravne omejitve. Če preizkuševalci ne morejo doseči načrtovane naslednje faze napada, jim mora nadzorna ekipa ob soglasju organa za TLPT občasno ponuditi pomoč. Taka pomoč na splošno pomeni pomoč v zvezi z informacijami in dostopom ter lahko vključuje zagotavljanje dostopa do sistemov IKT ali notranjih omrežij, da se testiranje lahko nadaljuje in se osredotoči na naslednje korake napada.

(23) Med aktivnim testiranjem rdeče ekipe bi bilo treba v fazi testiranja v primeru, da je to potrebno za nadaljevanje TLPT, kot zadnjo možnost v izjemnih okoliščinah in ko so bile izčrpane vse druge možnosti, izvesti dejavnost sodelovalnega testiranja, v katero bi bili vključeni tako preizkuševalci kot modra ekipa. V okviru tako omejenega povezovanja v vijolično ekipo se lahko uporabijo naslednje metode: „ulovi in izpusti“, pri kateri poskušajo preizkuševalci nadaljevati scenarije, so odkriti in nato nadaljujejo testiranje, „vojne igre“, ki omogočajo kompleksnejše scenarije za testiranje strateškega odločanja, ali „sodelovalna potrditev koncepta“, ki preizkuševalcem in članom modre ekipe omogoča, da skupaj potrdijo posebne varnostne ukrepe, orodja ali tehnike v nadzorovanem in sodelovalnem okolju.

(24) TLPT bi bilo treba uporabiti kot učno izkušnjo za krepitev digitalne operativne odpornosti finančnih subjektov. V zvezi s tem bi morali modra ekipa in preizkuševalci ponoviti napad in pregledati ukrepe, ki so bili sprejeti, da bi se iz testiranja učili v sodelovanju s preizkuševalci. V ta namen in da se omogoči ustrezna priprava, bi bilo treba pred izvajanjem kakršnih koli dejavnosti ponovitve vsem stranem, vključenim v dejavnosti ponovitve, dati na voljo poročilo o testiranju rdeče ekipe in poročilo o testiranju modre ekipe. Poleg tega bi bilo treba v zaključni fazi izvesti povezovanje v vijolično ekipo, da bi čim bolj okrepili učno izkušnjo. Metode, ki se lahko uporabijo za povezovanje v vijolično ekipo v zaključni fazi, bi morale vključevati razprave o alternativnih scenarijih napada, raziskovanje alternativnih scenarijev na aktivnih sistemih ali ponovno raziskovanje načrtovanih scenarijev na aktivnih sistemih, ki jih preizkuševalci v fazi testiranja niso mogli dokončati ali izvesti.

(25) Da bi se dodatno olajšala učna izkušnja vseh strani, vključenih v TLPT, v korist prihodnjih testiranj in da bi se okrepila digitalna operativna odpornost finančnih subjektov, bi si morale zadevne strani medsebojno zagotoviti povratne informacije o celotnem postopku in zlasti opredeliti, katere dejavnosti so dobro napredovale ali bi jih bilo mogoče izboljšati in kateri vidiki postopka TLPT so dobro delovali ali bi jih bilo mogoče izboljšati.

(26) Pristojni organi iz člena 46 Uredbe (EU) 2022/2554 in organi za TLPT, kadar so različni, bi morali sodelovati pri vključevanju naprednega testiranja na podlagi TLPT v obstoječe nadzorne postopke. V zvezi s tem in za skupno pravilno razumevanje ugotovitev TLPT in njihove razlage je primerno, da se zlasti za zbirno poročilo o testiranju in sanacijske načrte vzpostavi tesno sodelovanje med vodji testiranja, ki so bili vključeni v TLPT, in odgovornimi nadzorniki.

(27) Člen 26(8), prvi pododstavek, Uredbe (EU) 2022/2554 od finančnih subjektov zahteva, da sklenejo pogodbo z zunanjim preizkuševalcem za vsak tretji test. Kadar finančni subjekti v ekipo preizkuševalcev vključijo notranje in zunanje preizkuševalce, bi bilo treba to za namene navedenega člena šteti za TLPT, ki se izvaja z notranjimi preizkuševalci.

(28) Ta uredba temelji na osnutku regulativnih tehničnih standardov, ki so ga Komisiji predložili Evropski bančni organ, Evropski organ za zavarovanja in poklicne pokojnine ter Evropski organ za vrednostne papirje in trge (v nadaljnjem besedilu: evropski nadzorni organi) v dogovoru z Evropsko centralno banko.

(29) Evropski nadzorni organi so o osnutku regulativnih tehničnih standardov, na katerem temelji ta uredba, opravili odprta javna posvetovanja, analizirali morebitne s tem povezane stroške in koristi ter prosili za nasvet interesno skupino za bančništvo, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([3]), interesno skupino za zavarovanja in pozavarovanja ter interesno skupino za poklicne pokojninske sklade, ustanovljeni v skladu s členom 37 Uredbe (EU) št. 1094/2010 Evropskega parlamenta in Sveta ([4]), ter interesno skupino za vrednostne papirje in trge, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1095/2010 Evropskega parlamenta in Sveta ([5]).

(30) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([6]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 20. avgusta 2024 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „nadzorna ekipa“ pomeni ekipo, ki jo sestavljajo zaposleni pri finančnem subjektu, v katerem poteka testiranje, in, kadar je ustrezno, ob upoštevanju obsega penetracijskega testiranja na podlagi analize groženj (v nadaljnjem besedilu: TLPT), zaposleni pri njegovih tretjih ponudnikih storitev in katera koli druga stran, ki vodi testiranje;

(2) „vodja nadzorne ekipe“ pomeni zaposlenega pri finančnem subjektu, ki je odgovoren za izvedbo vseh dejavnosti, povezanih s TLPT, za finančni subjekt v okviru določenega testiranja;

(3) „modra ekipa“ pomeni zaposlene pri finančnem subjektu in, kadar je ustrezno, zaposlene pri tretjih ponudnikih storitev finančnega subjekta ter katero koli drugo stran, ki se šteje za pomembno glede na obseg TLPT, tretjih ponudnikov storitev finančnega subjekta, ki ščitijo uporabo omrežnih in informacijskih sistemov s strani finančnega subjekta tako, da ohranjajo njegovo varnostno stanje pred simuliranimi ali resničnimi napadi, in ki niso seznanjeni s TLPT;

(4) „naloge modre ekipe“ pomenijo naloge, ki jih običajno izvaja modra ekipa, kot so center za varnostne operacije, infrastrukturne storitve IKT, storitve službe za pomoč uporabnikom in storitve obvladovanja incidentov na operativni ravni;

(5) „rdeča ekipa“ pomeni preizkuševalce, notranje ali zunanje, s katerimi se sklene pogodba ali ki so dodeljeni za TLPT;

(6) „povezovanje v vijolično ekipo“ pomeni dejavnost sodelovalnega testiranja, ki vključuje preizkuševalce in modro ekipo;

([3]) Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES (UL L 331, 15.12.2010, str. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(7) „organ za TLPT“ pomeni kar koli od naslednjega:

(a) en sam javni organ v finančnem sektorju, imenovan v skladu s členom 26(9) Uredbe (EU) 2022/2554;

(b) organ v finančnem sektorju, na katerega se prenese izvajanje nekaterih ali vseh nalog v zvezi s TLPT v skladu s členom 26(10) Uredbe (EU) 2022/2554;

(c) kateri koli pristojni organ iz člena 46 Uredbe (EU) 2022/2554;

(8) „kibernetska ekipa za TLPT“ pomeni zaposlene pri organih za TLPT, ki so odgovorni za zadeve, povezane s TLPT;

(9) „vodje testiranja“ pomenijo zaposlene, imenovane za vodenje dejavnosti organa za TLPT za določen TLPT za spremljanje skladnosti s to uredbo;

(10) „ponudnik obveščevalnih podatkov o grožnjah“ pomeni strokovnjake, s katerimi finančni subjekt sklene pogodbo za vsak TLPT, nepovezane s finančnim subjektom in morebitnimi ponudniki storitev IKT znotraj skupine, ki zbirajo in analizirajo ciljno usmerjene obveščevalne podatke o grožnjah, pomembne za finančne subjekte v okviru posameznega izvajanja TLPT, ter pripravijo ustrezne relevantne in realistične scenarije groženj;

(11) „ponudniki TLPT“ pomenijo preizkuševalce in ponudnike obveščevalnih podatkov o grožnjah;

(12) „pomoč“ pomeni pomoč ali informacije, ki jih nadzorna ekipa zagotovi preizkuševalcem, da slednji lahko nadaljujejo izvajanje napadne poti, kadar sami ne morejo napredovati in kadar ni druge razumne alternative, med drugim zaradi pomanjkanja časa ali virov v določenem TLPT;

(13) „napadna pot“ pomeni pot, ki ji preizkuševalci sledijo v fazi aktivnega testiranja rdeče ekipe v okviru TLPT, da dosežejo oznake, določene za ta TLPT;

(14) „oznake“ so ključni cilji sistemov IKT, ki podpirajo kritične ali pomembne funkcije finančnega subjekta, ki jih preizkuševalci poskušajo doseči s testiranjem;

(15) „občutljive informacije“ pomenijo informacije, ki jih je mogoče zlahka izkoristiti za izvajanje napadov na sisteme IKT finančnega subjekta, intelektualno lastnino, zaupne poslovne podatke ali osebne podatke, ki lahko neposredno ali posredno škodujejo finančnemu subjektu in njegovemu ekosistemu, če bi prišle v roke zlonamernih akterjev;

(16) „skupina“ pomeni vse finančne subjekte, ki sodelujejo v skupnem TLPT v skladu s členom 26(4) Uredbe (EU) 2022/2554;

(17) „država članica gostiteljica“ pomeni državo članico gostiteljico v skladu s sektorskim pravom Unije, ki se uporablja za vsak finančni subjekt;

(18) „skupinski TLPT“ pomeni TLPT, ki ni skupni TLPT iz člena 26(4) Uredbe (EU) 2022/2554 in ki vključuje več finančnih subjektov, ki uporabljajo istega ponudnika storitev IKT znotraj skupine ali pripadajo isti skupini in uporabljajo skupne sisteme IKT.

Člen 2

Opredelitev finančnih subjektov, ki morajo izvajati TLPT

1. Organi za TLPT ocenijo, ali mora finančni subjekt izvajati TLPT, ob upoštevanju vpliva teh finančnih subjektov, njihovega sistemskega značaja in profila tveganja na področju IKT, na podlagi vseh naslednjih meril:

(a) dejavniki, povezani z vplivom in sistemskim značajem:

(i) velikost finančnega subjekta, določena na podlagi tega, ali finančni subjekt opravlja finančne storitve v eni ali več državah članicah, in s primerjavo dejavnosti finančnega subjekta z dejavnostmi drugih finančnih subjektov, ki opravljajo podobne storitve;

(ii) obseg in narava medsebojne povezanosti finančnega subjekta z drugimi finančnimi subjekti v finančnem sektorju v eni ali več državah članicah;

(iii) kritičnost ali pomen storitev, ki jih finančni subjekt zagotavlja finančnemu sektorju;

(iv) nadomestljivost storitev, ki jih opravlja finančni subjekt;

(v) kompleksnost poslovnega modela finančnega subjekta ter povezanih storitev in postopkov;

(vi) ali je finančni subjekt del skupine sistemskega značaja na ravni Unije ali nacionalni ravni v finančnem sektorju in uporablja skupne sisteme IKT;

(b) dejavniki, povezani s tveganji na področju IKT:

(i) profil tveganja finančnega subjekta;

(ii) krajina groženj finančnega subjekta;

(iii) stopnja odvisnosti kritičnih ali pomembnih funkcij ali njihovih podpornih funkcij finančnega subjekta od sistemov in postopkov IKT;

(iv) zapletenost arhitekture IKT finančnega subjekta;

(v) storitve in funkcije IKT, ki jih podpirajo tretji ponudniki storitev IKT, ter količina in vrsta pogodbenih dogovorov s tretjimi ponudniki storitev IKT ali ponudniki storitev IKT znotraj skupine;

(vi) rezultati vseh nadzornih pregledov, ki so pomembni za oceno zrelosti finančnega subjekta na področju IKT;

(vii) zrelost načrtov neprekinjenega poslovanja na področju IKT ter načrtov odzivanja in okrevanja IKT;

(viii) zrelost operativnih varnostnih ukrepov za odkrivanje in zmanjševanje tveganj na področju IKT, vključno z zmožnostjo:

(1) stalnega spremljanja infrastrukture IKT finančnega subjekta;

(2) odkrivanja dogodkov, povezanih z IKT, v realnem času;

(3) analiziranja dogodkov iz točke 2;

(4) pravočasnega in učinkovitega odzivanja na dogodke iz točke 2;

(ix) ali je finančni subjekt del skupine, dejavne v finančnem sektorju na ravni Unije ali nacionalni ravni, ki uporablja skupne sisteme IKT.

Za namene točke (a)(i) organ za TLPT, kadar je to mogoče, upošteva:

(a) tržni delež finančnega subjekta na ravni Unije in nacionalni ravni;

(b) nabor dejavnosti, ki jih ponuja finančni subjekt;

(c) tržni delež storitev, ki jih opravlja finančni subjekt, ali dejavnosti, ki jih izvaja na ravni Unije in nacionalni ravni.

Za namene točke (a)(v) organ za TLPT, kadar je to mogoče, upošteva:

(a) ali finančni subjekt uporablja več kot en poslovni model;

(b) medsebojno povezanost različnih poslovnih procesov in povezanih storitev.

2. Organi za TLPT zahtevajo, da vsi naslednji finančni subjekti izvajajo TLPT, razen če ocena iz odstavka 1 v zvezi s finančnim subjektom pokaže, da njegov vpliv, pomisleki glede finančne stabilnosti v zvezi s tem finančnim subjektom ali njegov profil tveganja na področju IKT ne upravičuje izvedbe TLPT:

(a) kreditne institucije, ki izpolnjujejo katerega koli od naslednjih pogojev:

(i) bile so opredeljene kot globalne sistemsko pomembne institucije (GSPI) v skladu s členom 131 Direktive 2013/36/EU Evropskega parlamenta in Sveta ([7]);

(ii) bile so opredeljene kot druge sistemsko pomembne institucije (DSPI) v skladu s členom 131 Direktive 2013/36/EU;

(iii) so del GSPI ali DSPI;

([7]) Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

(b) plačilne institucije, ki so v vsakem od dveh koledarskih let pred oceno organa za TLPT presegle 150 milijard EUR skupne vrednosti plačilnih transakcij, kot so opredeljene v členu 4, točka 5, Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta ([8]);

(c) institucije za izdajo elektronskega denarja, ki so v vsakem od dveh koledarskih let pred oceno organa za TLPT presegle 150 milijard EUR skupne vrednosti plačilnih transakcij, kot so opredeljene v členu 4, točka 5, Direktive (EU) 2015/2366, ali 40 milijard EUR skupne vrednosti zneska elektronskega denarja v obtoku;

(d) centralne depotne družbe;

(e) centralne nasprotne stranke;

(f) mesta trgovanja z elektronskim sistemom trgovanja, ki izpolnjujejo katero koli od naslednjih meril:

(i) mesto trgovanja ima največji tržni delež v smislu prometa na nacionalni ravni v vsakem od dveh koledarskih let pred oceno organa za TLPT na katerem koli od naslednjih področij:

(1) prenosljivi vrednostni papirji, kot so opredeljeni v členu 4(1), točka 44(a), Direktive 2014/65/EU Evropskega parlamenta in Sveta ([9]);

(2) prenosljivi vrednostni papirji, kot so opredeljeni v členu 4(1), točka 44(b), Direktive 2014/65/EU;

(3) izvedeni finančni instrumenti, kot so opredeljeni v členu 2(1), točka 29, Uredbe (EU) št. 600/2014 Evropskega parlamenta in Sveta ([10]);

(4) strukturirani finančni produkti, kot so opredeljeni v členu 2(1), točka 28, Uredbe (EU) št. 600/2014;

(5) pravice do emisije iz oddelka C, točka 11, Priloge I k Direktivi 2014/65/EU;

(ii) tržni delež mesta trgovanja v smislu prometa na ravni Unije v vsakem od dveh koledarskih let pred oceno organa za TLPT presega 5 % na katerem koli od naslednjih področij:

(1) delnice družb in drugi vrednostni papirji, enakovredni delnicam v podjetjih, partnerskih podjetjih ali drugih subjektih, ter potrdila o lastništvu v zvezi z delnicami;

(2) obveznice ali druge oblike listinjenega dolga, vključno s potrdili o lastništvu v zvezi s takimi vrednostnimi papirji;

(3) izvedeni finančni instrumenti, kot so opredeljeni v členu 2(1), točka 29, Uredbe (EU) št. 600/2014;

(4) strukturirani finančni produkti, kot so opredeljeni v členu 2(1), točka 28, Uredbe (EU) št. 600/2014;

(5) pravice do emisije iz oddelka C, točka 11, Priloge I k Direktivi 2014/65/EU;

([8]) Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L 337, 23.12.2015, str. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Uredba (EU) št. 600/2014 Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov in spremembi Uredbe (EU) št. 648/2012 (UL L 173, 12.6.2014, str. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

(g) zavarovalnice in pozavarovalnice, ki izpolnjujejo vsa naslednja merila:

(i) imajo bruto obračunano premijo, ki presega 1 500 000 000 EUR;

(ii) imajo zavarovalno-tehnične rezervacije, ki presegajo 10 000 000 000 EUR;

(iii) zavarovalnice, ki opravljajo samo dejavnosti življenjskega zavarovanja ali opravljajo dejavnosti življenjskega in neživljenjskega zavarovanja in katerih skupna sredstva presegajo 3,5 % vsote skupnih sredstev, vrednotenih v skladu s členom 75 Direktive 2009/138/ES Evropskega parlamenta in Sveta ([11]), zavarovalnic in pozavarovalnic s sedežem v državi članici.

Za namene točke (f)(ii), kadar je mesto trgovanja del skupine, ki uporablja skupne sisteme IKT ali istega ponudnika storitev IKT znotraj skupine, se upošteva promet pogodb o vrednostnih papirjih in izvedenih finančnih instrumentih na vseh mestih trgovanja, ki spadajo v isto skupino in imajo sedež v Uniji.

Za namene točke (g) organi za TLPT opredelijo podskupino vseh zavarovalnic in pozavarovalnic z uporabo meril iz točk (g)(i), (ii) in (iii). Od zavarovalnic in pozavarovalnic, vključenih v to podskupino, se zahteva, da izvajajo TLPT, če izpolnjujejo tudi katero koli od naslednjih meril:

(a) imajo bruto obračunano premijo, ki presega 3 000 000 000 EUR;

(b) imajo zavarovalno-tehnične rezervacije, ki presegajo 30 000 000 000 EUR;

(c) njihova skupna sredstva presegajo 10 % vsote skupnih sredstev, vrednotenih v skladu s členom 75 Direktive 2009/138/ES, zavarovalnic in pozavarovalnic s sedežem v državi članici.

3. Kadar več kot en finančni subjekt, ki pripada isti skupini in uporablja skupne sisteme IKT, ali več kot en finančni subjekt, ki uporablja istega ponudnika storitev IKT znotraj skupine, izpolnjuje merila iz odstavka 2, organi za TLPT teh finančnih subjektov v skladu s členom 16(2) odločijo, ali je zahteva za izvajanje TLPT na posamični podlagi ustrezna za te finančne subjekte.

Kadar se organ za TLPT obvladujočega podjetja skupine finančnih subjektov iz prvega pododstavka razlikuje od organov za TLPT finančnih subjektov skupine, se organi za TLPT finančnih subjektov, ki pripadajo tej skupini, s tem organom posvetujejo o tem, ali je primerno izvesti TLPT na posamični podlagi.

Člen 3

Vodje testiranj kibernetske ekipe za TLPT in TLPT

1. Organ za TLPT dodeli odgovornost za usklajevanje dejavnosti, povezanih s TLPT, kibernetski ekipi za TLPT. Kibernetsko ekipo za TLPT sestavljajo vodje testiranja, ki so dodeljeni za nadzor posameznega TLPT.

2. Organ za TLPT za vsako testiranje imenuje vodjo testiranja in vsaj enega namestnika.

3. Vodje testiranja spremljajo, ali so izpolnjene zahteve iz te uredbe, in zagotovijo njihovo izpolnjevanje.

([11]) Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Vodja testiranja finančnemu subjektu sporoči kontaktne podatke kibernetske ekipe za TLPT z obvestilom iz člena 9(1).

5. Organ za TLPT sodeluje v vseh fazah TLPT.

Člen 4

Organizacijska ureditev za finančne subjekte

1. Finančni subjekti imenujejo vodjo nadzorne ekipe, ki je odgovoren za vsakodnevno vodenje TLPT ter za odločitve in ukrepe nadzorne ekipe.

2. Finančni subjekti sprejmejo organizacijske in postopkovne ukrepe za zagotovitev, da:

(a) je dostop do informacij v zvezi z načrtovanim ali potekajočim TLPT omejen na podlagi potrebe po seznanitvi na nadzorno ekipo, upravljalni organ, preizkuševalce, ponudnika obveščevalnih podatkov o grožnjah in organ za TLPT;

(b) se nadzorna ekipa pred vključitvijo katerega koli člana modre ekipe v TLPT posvetuje z vodji testiranja;

(c) je nadzorna ekipa obveščena o vsakem odkritju TLPT s strani zaposlenih pri finančnem subjektu ali njegovih tretjih ponudnikih storitev; nadzorna ekipa v primeru eskalacije posledičnega odziva na incident po potrebi tako stopnjevanje umiri;

(d) so vzpostavljene ureditve v zvezi s tajnostjo TLPT, ki velja za zaposlene pri finančnem subjektu, zaposlene pri zadevnih tretjih ponudnikih storitev IKT, preizkuševalce in ponudnika obveščevalnih podatkov o grožnjah;

(e) nadzorna ekipa vodjem testiranja na zahtevo zagotovi vse informacije v zvezi s TLPT;

(f) kadar je mogoče, strani, vključene v TLPT, za vse omembe slednjega uporabljajo šifro.

Člen 5

Obvladovanje tveganj pri TLPT

1. Nadzorna ekipa v pripravljalni fazi iz člena 9 oceni tveganja, povezana s testiranjem aktivnih produkcijskih sistemov s kritičnimi ali pomembnimi funkcijami finančnega subjekta, vključno z morebitnimi vplivi na:

(a) finančni sektor;

(b) finančno stabilnost na ravni Unije ali nacionalni ravni.

Nadzorna ekipa te vplive pregleduje med celotnim testiranjem.

2. Nadzorna ekipa za namene ocene in obvladovanja tveganj upošteva vsaj naslednje vrste tveganj, povezanih z:

(a) omogočanjem dostopa do občutljivih informacij o finančnem subjektu ponudniku obveščevalnih podatkov o grožnjah in, kadar je ustrezno, zunanjim preizkuševalcem;

(b) neskladnostjo TLPT z Uredbo (EU) 2022/2554 in to uredbo, kadar zaradi take neskladnosti ni izdano potrdilo iz člena 26(7) Uredbe (EU) 2022/2554, tudi kadar je do take neskladnosti prišlo zaradi kršitev zaupnosti TLPT ali neetičnega ravnanja;

(c) eskalacijo kriz in incidentov;

(d) fazo aktivne rdeče ekipe, vključno s tveganji, povezanimi s prekinitvijo kritičnih dejavnosti in okvaro podatkov zaradi dejavnosti preizkuševalcev, ter njenimi morebitnimi učinki na tretje osebe;

(e) dejavnostjo modre ekipe, vključno s tveganji, povezanimi s prekinitvijo kritičnih dejavnosti in okvaro podatkov zaradi dejavnosti modre ekipe, ter njenimi morebitnimi učinki na tretje osebe;

(f) nepopolno obnovitvijo sistemov, ki jih je prizadel TLPT.

Člen 6

Obvladovanje tveganj pri skupnem ali skupinskem TLPT

1. V primeru skupinskega TLPT ali skupnega TLPT nadzorna ekipa vsakega finančnega subjekta izvede lastno oceno tveganj in sprejme lastne ukrepe za obvladovanje tveganj.

2. Nadzorna ekipa imenovanega finančnega subjekta iz člena 16(3), točka (b), te uredbe ali finančnega subjekta, imenovanega v skladu s členom 26(4) Uredbe (EU) 2022/2554, oceni tveganja v zvezi z vključenostjo več finančnih subjektov v TLPT. Nadzorne ekipe vključenih finančnih subjektov sodelujejo z nadzorno ekipo imenovanega finančnega subjekta, da odkrijejo morebitna skupna tveganja.

Člen 7

Izbira ponudnikov TLPT

1. Nadzorna ekipa sprejme ukrepe za obvladovanje tveganj v zvezi s TLPT in zlasti zagotovi, da za vsak TLPT:

(a) ponudnik obveščevalnih podatkov o grožnjah in zunanji preizkuševalci nadzorni ekipi predložijo podroben življenjepis in kopije certificiranj, ki so v skladu s priznanimi tržnimi standardi primerna za izvajanje njihovih dejavnosti;

(b) ponudnik obveščevalnih podatkov o grožnjah in zunanji preizkuševalci imajo ustrezno in polno kritje z ustreznimi zavarovanji poklicne odgovornosti, vključno s kritjem tveganja kršitve in malomarnosti;

(c) ponudnik obveščevalnih podatkov o grožnjah predloži vsaj tri reference iz prejšnjih nalog na področju TLPT in testiranja rdeče ekipe;

(d) zunanji preizkuševalci predložijo vsaj pet referenc iz prejšnjih nalog, povezanih s TLPT in testiranjem rdeče ekipe;

(e) ponudnik obveščevalnih podatkov o grožnjah za TLPT dodeli zaposlene, ki:

(i) obsegajo najmanj vodjo, ki ima najmanj pet let izkušenj na področju obveščevalnih podatkov o grožnjah, in najmanj enega dodatnega člana, ki ima najmanj dve leti izkušenj na področju obveščevalnih podatkov o grožnjah;

(ii) izkazujejo široko paleto in ustrezno raven strokovnega znanja in spretnosti, ki vključujejo:

(1) taktike, tehnike in postopke zbiranja obveščevalnih podatkov;

(2) geopolitično, tehnično in sektorsko znanje;

(3) ustrezne komunikacijske spretnosti za jasno predstavitev rezultatov sodelovanja in poročanje o njih;

(iii) imajo kombinirano udeležbo v najmanj treh prejšnjih nalogah na področju obveščevalnih podatkov o grožnjah v okviru penetracijskega testiranja in testiranja rdeče ekipe;

(iv) hkrati ne opravljajo nalog modre ekipe ali drugih storitev, ki bi lahko pomenile nasprotje interesov v zvezi s finančnim subjektom, tretjim ponudnikom storitev IKT ali ponudnikom storitev IKT znotraj skupine, vključenim v TLPT, za katerega so dodeljeni;

(v) so ločeni od zaposlenih istega ponudnika TLPT, ki zagotavlja zunanje preizkuševalce za isti TLPT, in jim ne poročajo;

(f) za zunanje preizkuševalce se za TLP dodeli rdeča ekipa, ki:

(i) obsega najmanj vodjo, ki ima najmanj pet let izkušenj s penetracijskim testiranjem in testiranjem rdeče ekipe, in najmanj dva dodatna preizkuševalca, od katerih ima vsak najmanj dve leti izkušenj s penetracijskim testiranjem in testiranjem rdeče ekipe;

(ii) izkazuje široko paleto in ustrezno raven strokovnega znanja in spretnosti, vključno s poznavanjem poslovanja finančnega subjekta, izvidništva, obvladovanja tveganj, razvoja programov za izkoriščanje ranljivosti, fizičnega vdora, socialnega inženiringa in analize ranljivosti ter ustreznimi komunikacijskimi spretnostmi za jasno predstavitev rezultatov sodelovanja in poročanje o njih;

(iii) ima kombinirano udeležbo v najmanj petih prejšnjih nalogah, povezanih s penetracijskim testiranjem in testiranjem rdeče ekipe;

(iv) ni zaposlena pri ponudniku obveščevalnih podatkov o grožnjah, ki hkrati opravlja naloge modre ekipe za finančni subjekt, tretjega ponudnika storitev IKT ali ponudnika storitev IKT znotraj skupine, ki je vključen v TLPT, in zanj ne opravlja storitev;

(v) je ločena od zaposlenih pri istem ponudniku TLPT, ki hkrati opravlja storitve obveščanja o grožnjah v okviru istega TLPT;

(g) preizkuševalci in ponudnik obveščevalnih podatkov o grožnjah ob koncu testiranja izvedejo postopke za obnovitev, vključno z varnim izbrisom informacij v zvezi z gesli, poverilnicami in drugimi tajnimi ključi, ki so bili ogroženi med TLPT, varnim sporočanjem finančnim subjektom o ogroženih računih, varnim zbiranjem, shranjevanjem, upravljanjem in odstranjevanjem drugih podatkov, zbranih pri testiranju;

(h) preizkuševalci poleg postopkov za obnovitev ob koncu testiranja iz točke (g) izvedejo naslednje postopke za obnovitev:

(i) deaktiviranje poveljevanja in nadzora;

(ii) nastavitve obsega in datuma pri stikalih za izklop v sili;

(iii) odstranitev stranskih vrat in druge zlonamerne programske opreme;

(iv) obveščanje o morebitnih zlorabah;

(v) postopke za prihodnjo obnovitev iz varnostnih kopij, ki se lahko nanaša na zlonamerno programsko opremo ali orodja, nameščena med testiranjem;

(vi) spremljanje dejavnosti modre ekipe in obveščanje nadzorne ekipe o morebitnih odkritjih;

(i) preizkuševalci in ponudnik obveščevalnih podatkov o grožnjah ne izvajajo nobene od naslednjih dejavnosti in pri njih ne sodelujejo:

(i) nepooblaščeno uničenje opreme finančnega subjekta in njegovih tretjih ponudnikov storitev IKT, če obstajajo;

(ii) nenadzorovano spreminjanje informacijskih sredstev in sredstev IKT finančnega subjekta in njegovih tretjih ponudnikov storitev IKT, če obstajajo;

(iii) namerno ogrožanje neprekinjenosti kritičnih ali pomembnih funkcij finančnega subjekta;

(iv) nepooblaščena vključitev sistemov, ki ne spadajo v obseg testiranja;

(v) nepooblaščeno razkritje rezultatov testiranja.

2. Nadzorna ekipa vodi evidenco dokumentacije, ki jo predložijo preizkuševalci in ponudniki obveščevalnih podatkov o grožnjah, da dokaže skladnost z odstavkom 1, točke (a) do (f).

V izjemnih okoliščinah lahko finančni subjekti sklenejo pogodbo z zunanjimi preizkuševalci in ponudniki obveščevalnih podatkov o grožnjah, ki ne izpolnjujejo ene ali več zahtev iz odstavka 1, točke (a) do (f), če ti finančni subjekti sprejmejo ukrepe, ki so ustrezni za zmanjšanje tveganj, povezanih z neskladnostjo s takimi točkami, in te ukrepe evidentirajo.

Člen 8

Posebnosti pri skupnem ali skupinskem TLPT

1. Če vodilni organ za TLPT ne odloči drugače, kadar je v skupni ali skupinski TLPT vključenih več finančnih subjektov, opredeljenih v skladu s členom 16(2) ali (4), vsak finančni subjekt izvede vsakega od korakov iz členov 9 do 15.

2. Če v tej uredbi ni določeno drugače, kadar je v skupinski ali skupni TLPT vključenih več organov za TLPT iz člena 16(3) ali (5), se sklicevanja na „organ za TLPT“ v členih 9 do 15 razumejo kot sklicevanje na vodilni organ za TLPT za tak skupni ali skupinski TLPT.

Člen 9

Pripravljalna faza

1. Finančni subjekt, opredeljen v skladu s členom 26, odstavek (8), tretji pododstavek, Uredbe (EU) 2022/2554, začne TLPT po prejemu uradnega obvestila organa za TLPT, da mora izvesti TLPT.

2. Finančni subjekt v treh mesecih po prejemu obvestila iz odstavka 1 vodjem testiranja predloži vse naslednje informacije o začetku TLPT:

(a) projektno listino, vključno s projektnim načrtom na visoki ravni, ki vsebuje informacije iz Priloge I;

(b) kontaktne podatke vodje nadzorne ekipe;

(c) informacije o predvideni uporabi notranjih ali zunanjih preizkuševalcev ali obojih, kadar je to ustrezno, kot je navedeno v členu 15;

(d) informacije o komunikacijskih kanalih, ki se bodo uporabljali med TLPT;

(e) šifro za TLPT.

3. Kadar so informacije iz odstavka 2, točke (a) do (e), popolne ter zagotavljajo ustreznost in učinkovito izvajanje TLPT, organ za TLPT potrdi informacije o začetku TLPT finančnega subjekta in o tem uradno obvesti finančni subjekt.

4. Potem ko organ za TLPT potrdi informacije o začetku TLPT, finančni subjekt sestavi nadzorno ekipo za podporo vodji nadzorne ekipe pri njegovih nalogah, ki so:

(a) vzpostavitev komunikacijskih kanalov in postopkov znotraj nadzorne ekipe s preizkuševalci in ponudniki obveščevalnih podatkov o grožnjah v vseh zadevah v zvezi s TLPT;

(b) obveščanje upravljalnega organa finančnega subjekta o napredku TLPT in povezanih tveganjih;

(c) sprejemanje odločitev na podlagi strokovnega znanja na tem področju med celotnim potekom TLPT;

(d) izvajanje TLPT v skladu s to uredbo;

(e) izbira ponudnika obveščevalnih podatkov o grožnjah za TLPT;

(f) izbira zunanjih preizkuševalcev, notranjih preizkuševalcev ali obojih;

(g) priprava dokumenta s specifikacijo obsega.

5. Kadar organ za TLPT meni, da so začetna sestava nadzorne ekipe in vse njene naknadne spremembe ustrezne za izvajanje nalog iz odstavka 4, potrdi nadzorno ekipo in o tem uradno obvesti njenega vodjo.

6. Finančni subjekt vodjem testiranja v šestih mesecih od prejema uradnega obvestila organa za TLPT iz odstavka 1 predloži dokument s specifikacijo obsega, ki vsebuje vse informacije iz Priloge II. Upravljalni organ finančnega subjekta odobri dokument s specifikacijo obsega.

7. Finančni subjekti upoštevajo naslednja merila za vključitev kritičnih ali pomembnih funkcij v obseg TLPT:

(a) kritičnost ali pomembnost funkcije in njen morebitni vpliv na finančni sektor in finančno stabilnost na ravni Unije in nacionalni ravni;

(b) pomembnost funkcije za vsakodnevno poslovanje finančnega subjekta;

(c) zamenljivost funkcije;

(d) medsebojna povezanost z drugimi funkcijami;

(e) geografska lokacija funkcije;

(f) odvisnost drugih subjektov v sektorju od funkcije;

(g) obveščevalni podatki o grožnjah v zvezi s funkcijo, če so na voljo.

8. Nadzorna ekipa preizkuševalcem in ponudnikom obveščevalnih podatkov o grožnjah posreduje informacije o začetku TLPT in dokument s specifikacijo obsega, ko je z njimi sklenjena pogodba. Nadzorna ekipa obvesti preizkuševalce in ponudnike obveščevalnih podatkov o grožnjah o postopku testiranja, ki ga je treba upoštevati.

9. Finančni subjekt zagotovi, da se pridobitev ali dodelitev preizkuševalcev in ponudnikov obveščevalnih podatkov o grožnjah zaključi pred začetkom faze testiranja.

10. Pred začetkom faze testiranja se nadzorna ekipa z vodji testiranja posvetuje o oceni tveganj TLPT in ukrepih za obvladovanje tveganj. Nadzorna ekipa ponovno pregleda oceno tveganj ali ukrepe za obvladovanje tveganj, kadar organ za TLPT meni, da ne obravnavajo ustrezno tveganj TLPT.

11. Nadzorna ekipa oceni skladnost ponudnikov obveščevalnih podatkov o grožnjah in preizkuševalcev, ki jih namerava vključiti v TLPT, z zahtevami iz člena 27 Uredbe (EU) 2022/2554 in s členom 7(1) te uredbe ter dokumentira rezultat te ocene. Nadzorna ekipa izbere ponudnike obveščevalnih podatkov o grožnjah v skladu s to oceno in svojimi praksami obvladovanja tveganj. Nadzorna ekipa pred sklenitvijo pogodbe z izbranimi ponudniki obveščevalnih podatkov o grožnjah in zunanjimi preizkuševalci vodjem testiranja zagotovi dokaze o skladnosti teh ponudnikov obveščevalnih podatkov o grožnjah in preizkuševalcev z zahtevami iz člena 27 Uredbe (EU) 2022/2554 in člena 7(1) te uredbe. Nadzorna ekipa ne sklene pogodbe z izbranimi ponudniki obveščevalnih podatkov o grožnjah in zunanjimi preizkuševalci, kadar organ za TLPT meni, da izbrani ponudniki obveščevalnih podatkov o grožnjah in zunanji preizkuševalci ne izpolnjujejo zahtev iz člena 27 Uredbe (EU) 2022/2554 ali zahtev iz člena 7(1) te uredbe ali dodatnih zahtev, ki izhajajo iz nacionalne zakonodaje o varnosti v skladu s pravom Unije, ali kadar finančni subjekt ne izpolnjuje zahtev iz člena 7(2), prvi pododstavek, te uredbe ali kadar okoliščine iz člena 7(2), drugi pododstavek, te uredbe niso izpolnjene.

12. Kadar je dokument s specifikacijo obsega popoln in zagotavlja izvajanje ustreznega in učinkovitega TLPT, organ za TLPT dokument odobri in o tem obvesti vodjo nadzorne ekipe.

Člen 10

Faza testiranja: obveščevalni podatki o grožnjah

1. Potem ko organ za TLPT odobri dokument s specifikacijo obsega, ponudnik obveščevalnih podatkov o grožnjah analizira splošne in sektorske obveščevalne podatke o grožnjah, ki so pomembni za finančni subjekt. Kadar organ za TLPT zagotovi splošno krajino groženj za finančni sektor države članice, lahko ponudnik obveščevalnih podatkov o grožnjah to krajino uporabi kot izhodišče za nacionalno krajino groženj. Ponudnik obveščevalnih podatkov o grožnjah opredeli kibernetske grožnje in obstoječe ali morebitne ranljivosti v zvezi s finančnim subjektom. Poleg tega ponudnik obveščevalnih podatkov o grožnjah zbira informacije o konkretnih in kontekstualiziranih obveščevalnih podatkih o tarčah in grožnjah v zvezi s finančnim subjektom, na podlagi katerih je mogoče ukrepati, ter jih analizira, tudi s posvetovanjem z nadzorno ekipo in vodji testiranja.

2. Ponudnik obveščevalnih podatkov o grožnjah nadzorni ekipi, preizkuševalcem in vodjem testiranja predstavi ustrezne grožnje in ciljno usmerjene obveščevalne podatke o grožnjah ter predlaga potrebne scenarije. Predlagani scenariji se razlikujejo glede na opredeljene akterje groženj ter povezane taktike, tehnike in postopke ter so usmerjeni v vsako kritično ali pomembno funkcijo, ki je vključena v obseg TLPT.

3. Vodja nadzorne ekipe izbere vsaj tri scenarije za izvedbo TLPT na podlagi vseh naslednjih elementov:

(a) priporočilo ponudnika obveščevalnih podatkov o grožnjah in narava vsakega scenarija na podlagi groženj;

(b) podatki, ki jih zagotovijo vodje testiranja;

(c) izvedljivost predlaganih scenarijev za izvedbo na podlagi strokovne presoje preizkuševalcev;

(d) velikost, kompleksnost in splošni profil tveganja finančnega subjekta ter narava, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja.

4. Največ eden od izbranih scenarijev lahko namesto na analizi groženj temelji na v prihodnost usmerjeni in potencialno navidezni grožnji z visoko napovedno, anticipativno, oportunistično ali potencialno vrednostjo glede na pričakovani razvoj krajine groženj v zvezi s finančnim subjektom.

Pri skupnem TLPT, brez poseganja v scenarije, ki so neposredno usmerjeni v kritične ali pomembne funkcije finančnih subjektov, vključenih v testiranje, najmanj en scenarij vključuje ustrezne osnovne sisteme, postopke in tehnologije IKT tretjega ponudnika storitev IKT, ki podpirajo kritične ali pomembne funkcije finančnih subjektov, vključenih v obseg TLPT.

Pri skupinskem TLPT, v katerega je vključen ponudnik storitev IKT znotraj skupine, brez poseganja v scenarije, ki so neposredno usmerjeni v kritične ali pomembne funkcije finančnih subjektov, vključenih v testiranje, najmanj en scenarij vključuje ustrezne osnovne sisteme, postopke in tehnologije IKT ponudnika storitev IKT znotraj skupine, ki podpirajo kritične ali pomembne funkcije finančnih subjektov, vključenih v obseg TLPT.

5. Ponudnik obveščevalnih podatkov o grožnjah nadzorni ekipi predloži ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah, vključno s scenariji, izbranimi v skladu z odstavkoma 3 in 4. Poročilo o obveščevalnih podatkih o grožnjah vsebuje informacije iz Priloge III.

6. Nadzorna ekipa predloži ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah vodji testiranja v odobritev. Kadar je ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah popolno in zagotavlja izvajanje učinkovitega TLPT, organ za TLPT poročilo odobri in o tem obvesti vodjo nadzorne ekipe.

Člen 11

Faza testiranja: testiranje rdeče ekipe

1. Potem ko organ za TLPT odobri ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah, preizkuševalci pripravijo načrt testiranja rdeče ekipe, ki vsebuje informacije iz Priloge IV. Preizkuševalci kot podlago za pripravo scenarijev napada uporabijo dokument s specifikacijo obsega in ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah.

2. Preizkuševalci se posvetujejo z nadzorno ekipo, ponudnikom obveščevalnih podatkov o grožnjah in vodji testiranja o načrtu testiranja rdeče ekipe, vključno z dogovorom glede komuniciranja, postopkov in vodenja projektov, pripravo in primeri uporabe za aktivacijo pomoči ter dogovori o poročanju nadzorni ekipi in vodjem testiranja.

3. Kadar je načrt testiranja rdeče ekipe popoln in zagotavlja izvajanje učinkovitega TLPT, nadzorna ekipa in organ za TLPT odobrita načrt testiranja rdeče ekipe, organ za TLPT pa o tem obvesti vodjo nadzorne ekipe.

4. Po odobritvi načrta testiranja rdeče ekipe v skladu z odstavkom 3 preizkuševalci izvedejo TLPT v fazi aktivnega testiranja rdeče ekipe.

5. Trajanje faze aktivnega testiranja rdeče ekipe je sorazmerno z obsegom TLPT, obsegom, dejavnostjo, kompleksnostjo in številom finančnih subjektov in tretjih ponudnikov storitev IKT ali ponudnikov storitev IKT znotraj skupine, vključenih v TLPT, v vsakem primeru pa traja najmanj 12 tednov. Scenariji napada se lahko izvajajo zaporedno ali hkrati. Nadzorna ekipa, ponudnik obveščevalnih podatkov o grožnjah, preizkuševalci in vodje testiranja se dogovorijo o koncu faze aktivnega testiranja rdeče ekipe.

6. Ob zagotovitvi, da načrt testiranja rdeče ekipe ostane popoln in omogoča izvedbo učinkovitega TLPT, vodja nadzorne ekipe in vodje testiranja odobrijo vse spremembe načrta testiranja rdeče ekipe po njegovi odobritvi, vključno s časovnico, obsegom, ciljnimi sistemi ali oznakami.

7. V celotni fazi aktivnega testiranja rdeče ekipe preizkuševalci vsaj enkrat tedensko poročajo nadzorni ekipi in vodjem testiranja o napredku, doseženem pri TLPT, ponudnik obveščevalnih podatkov o grožnjah pa je še naprej na voljo za posvetovanje in dodatne obveščevalne podatke o grožnjah, kadar to zahteva nadzorna ekipa.

8. Nadzorna ekipa pravočasno zagotovi pomoč, zasnovano na podlagi načrta testiranja rdeče ekipe. Pomoč se lahko doda ali prilagodi po odobritvi nadzorne ekipe in vodij testiranja.

9. Če dejavnosti testiranja odkrije kateri koli zaposleni pri finančnem subjektu ali njegovih tretjih ponudnikih storitev IKT ali ponudniku storitev IKT znotraj skupine, kadar je to ustrezno, nadzorna ekipa v posvetovanju s preizkuševalci in brez poseganja v odstavek 10 predlaga ukrepe, ki omogočajo nadaljevanje TLPT ob zagotovitvi njegove tajnosti, in jih predloži vodjem testiranja v potrditev.

10. V izjemnih okoliščinah, ki povzročijo tveganja vpliva na podatke, škode na sredstvih in motenj kritičnih ali pomembnih funkcij, storitev ali poslovanja samega finančnega subjekta, njegovih tretjih ponudnikov storitev IKT ali ponudnikov storitev IKT znotraj skupine ali motenj pri nasprotnih strankah ali v finančnem sektorju, lahko vodja nadzorne ekipe začasno prekine TLPT ali v skrajnem primeru, kadar nadaljevanje TLPT drugače ni mogoče in ga mora predhodno potrditi organ za TLPT, nadaljuje TLPT z uporabo omejenega povezovanja v vijolično ekipo. Trajanje omejenega povezovanja v vijolično ekipo se šteje v najmanj 12-tedensko trajanja faze aktivnega testiranja rdeče ekipe iz odstavka 5.

Člen 12

Zaključna faza

1. Po koncu faze aktivnega testiranja rdeče ekipe vodja nadzorne ekipe obvesti modro ekipo, da je bil izveden TLPT.

2. V štirih tednih po koncu faze aktivnega testiranja rdeče ekipe preizkuševalci nadzorni ekipi predložijo poročilo o testiranju rdeče ekipe, ki vsebuje informacije iz Priloge V.

3. Nadzorna ekipa poročilo o testiranju rdeče ekipe brez nepotrebnega odlašanja predloži modri ekipi in vodjem testiranja.

Na zahtevo vodij testiranja poročilo iz prvega pododstavka ne vsebuje občutljivih informacij.

4. Modra ekipa po prejemu poročila o testiranju rdeče ekipe in najpozneje deset tednov po koncu faze aktivnega testiranja rdeče ekipe nadzorni ekipi predloži poročilo o testiranju modre ekipe, ki vsebuje informacije iz Priloge VI. Nadzorna ekipa poročilo o testiranju modre ekipe brez nepotrebnega odlašanja predloži preizkuševalcem in vodjem testiranja.

Na zahtevo vodij testiranja poročilo iz prvega pododstavka ne vsebuje občutljivih informacij.

5. Modra ekipa in preizkuševalci najpozneje deset tednov po koncu faze aktivnega testiranja rdeče ekipe ponovijo dejanja napada in obrambe, ki so bila izvedena med TLPT. Nadzorna ekipa izvede tudi povezovanje v vijolično ekipo za obravnavo tem, ki so jih skupaj opredelili modra ekipa in preizkuševalci, in sicer na podlagi ranljivosti, ugotovljenih med testiranjem, in, če je ustrezno, točk, ki jih ni bilo mogoče testirati v fazi aktivnega testiranja rdeče ekipe.

6. Nadzorna ekipa, modra ekipa, preizkuševalci in ponudniki obveščevalnih podatkov o grožnjah si po zaključku ponovitve in povezovanja v vijolično ekipo medsebojno podajo povratne informacije o postopku TLPT. Vodje testiranja lahko podajo povratne informacije.

7. Ko organ za TLPT uradno obvesti vodjo nadzorne ekipe, da je ocenil, da poročilo o testiranju modre ekipe in poročilo o testiranju rdeče ekipe vsebujeta informacije iz prilog V in VI, finančni subjekt organu za TLPT v osmih tednih v odobritev predloži poročilo, v katerem so povzete relevantne ugotovitve TLPT, kot je navedeno v členu 26(6) Uredbe (EU) 2022/2554, in ki vsebuje elemente iz Priloge VII.

Na zahtevo organa za TLPT poročilo iz prvega pododstavka ne vsebuje občutljivih informacij.

Člen 13

Sanacijski načrt

1. Finančni subjekt v osmih tednih od uradnega obvestila iz člena 12(7) te uredbe organu za TLPT in pristojnemu organu finančnega subjekta, kadar sta različna, predloži sanacijske načrte in dokumentacijo iz člena 26(6) Uredbe (EU) 2022/2554.

2. Sanacijski načrt iz odstavka 1 za vsako ugotovitev, ki izhaja iz TLPT, vključuje:

(a) opis ugotovljenih pomanjkljivosti;

(b) opis predlaganih sanacijskih ukrepov ter njihovo prednostno razvrstitev in pričakovani zaključek, kjer je primerno, vključno z ukrepi za izboljšanje zmožnosti za prepoznavanje, zaščito, odkrivanje in odzivanje;

(c) analizo temeljnih vzrokov;

(d) zaposlene pri finančnem subjektu ali funkcije finančnega subjekta, odgovorne za izvajanje predlaganih sanacijskih ukrepov ali izboljšav;

(e) tveganja, povezana z neizvajanjem ukrepov iz točke (b), in, če je ustrezno, tveganja, povezana z izvajanjem takih ukrepov.

Člen 14

Potrdilo

1. Potrdilo iz člena 26(7) Uredbe (EU) 2022/2554 vsebuje informacije iz Priloge VIII.

2. Kadar je bilo v TLPT vključenih več organov za TLPT, testiranim finančnim subjektom potrdilo iz člena 26(7) Uredbe (EU) 2022/2554 predloži vodilni organ za TLPT.

Člen 15

Uporaba notranjih preizkuševalcev

1. Finančni subjekti sprejmejo vse naslednje ureditve za uporabo notranjih preizkuševalcev:

(a) oblikovanje in izvajanje politike za vodenje notranjih preizkuševalcev v TLPT;

(b) ukrepe za zagotovitev, da uporaba notranjih preizkuševalcev za izvajanje TLPT ne vpliva negativno na splošne obrambne zmožnosti ali odpornost finančnega subjekta proti incidentom, ki so povezani z IKT, ali znatno vpliva na razpoložljivost virov, ki so namenjeni nalogam v zvezi z IKT, med TLPT;

(c) ukrepe za zagotovitev, da imajo notranji preizkuševalci dovolj virov in zmožnosti za izvajanje TLPT.

Politika iz točke (a):

(a) vsebuje merila za ocenjevanje ustreznosti, usposobljenosti in morebitnih nasprotij interesov notranjih preizkuševalcev ter določa vodstvene odgovornosti v postopku testiranja;

(b) se dokumentira in redno pregleduje;

(c) zagotovi, da ekipa notranjih preizkuševalcev vsebuje vodjo testiranja in najmanj dva dodatna člana;

(d) zahteva, da so bili vsi člani ekipe preizkuševalcev v predhodnih 12 mesecih zaposleni pri finančnem subjektu ali pri ponudniku storitev IKT znotraj skupine;

(e) vsebuje določbe glede usposabljanja notranjih preizkuševalcev o tem, kako se izvaja penetracijsko testiranje in testiranje rdeče ekipe.

2. Kadar organ za TLPT odobri uporabo notranjih preizkuševalcev v skladu s členom 27(2), točka (a), Uredbe (EU) 2022/2554, upošteva zahteve iz člena 7(1) te uredbe.

3. Finančni subjekt v primeru uporabe notranjih preizkuševalcev zagotovi, da je taka uporaba navedena v naslednjih dokumentih:

(a) informacijah o začetku testiranja iz člena 9;

(b) poročilu o testiranju rdeče ekipe iz člena 12(2);

(c) poročilu s povzetkom relevantnih ugotovitev TLPT iz člena 26(6) Uredbe (EU) 2022/2554.

4. Preizkuševalci, zaposleni pri ponudniku storitev IKT znotraj skupine, se štejejo za notranje preizkuševalce finančnega subjekta.

Člen 16

Sodelovanje in vzajemno priznavanje

1. Za namene izvajanja TLPT v zvezi s finančnim subjektom, ki opravlja storitve v več kot eni državi članici, tudi prek podružnice, njegov organ za TLPT:

(a) določi, kateri organi za TLPT v državah članicah gostiteljicah bodo vključeni, pri čemer upošteva, ali v državah članicah gostiteljicah deluje ena ali več kritičnih ali pomembnih funkcij ali si jo delijo;

(b) obvesti organe za TLPT, določene v skladu s točko (a), o odločitvi za izvedbo TLPT v finančnem subjektu;

(c) če se organi za TLPT ne dogovorijo drugače, TLPT vodi organ za TLPT finančnega subjekta.

Organi za TLPT držav članic gostiteljic lahko v 20 delovnih dneh od prejema informacije o prihodnjem izvajanju TLPT izrazijo svoj interes za spremljanje TLPT v vlogi opazovalcev ali imenujejo vodjo testiranja za sodelovanje v TLPT. Vodilni organ za TLPT vsem organom za TLPT, ki so prevzeli vlogo opazovalcev v TLPT, predloži dokument s specifikacijo obsega, zbirno poročilo o testiranju, sanacijski načrt in potrdilo.

Vodilni organ za TLPT med celotnim testiranjem usklajuje vse sodelujoče organe za TLPT ter sprejema vse odločitve, ki so potrebne za ustrezno in učinkovito izvajanje TLPT. Vodilni organ za TLPT lahko določi največje število sodelujočih organov za TLPT, če bi bilo sicer ogroženo učinkovito izvajanje TLPT.

2. Kadar finančni subjekt uporablja istega ponudnika storitev IKT znotraj skupine kot finančni subjekti s sedežem v drugih državah članicah ali pripada skupini in uporablja iste sisteme IKT kot finančni subjekti iste skupine s sedežem v drugih državah članicah, organ za TLPT finančnega subjekta stopi v stik z organi za TLPT drugih finančnih subjektov, ki uporabljajo istega ponudnika storitev IKT znotraj skupine ali v okviru skupine uporabljajo iste sisteme IKT, ter z njimi oceni izvedljivost in ustreznost izvajanja skupinskega TLPT za te finančne subjekte. Skupinski TLPT ima prednost pred posamičnim TLPT, kadar lahko pomeni manj stroškov in potrebnih virov za finančne subjekte in organe za TLPT, pod pogojem, da ne zmanjšuje zanesljivosti in učinkovitosti testiranja.

3. Za namene izvajanja skupinskega TLPT:

(a) se organi za TLPT finančnih subjektov dogovorijo o tem, kateri finančni subjekt bo določen za izvajanje TLPT, pri čemer upoštevajo strukturo skupine in učinkovitost testiranja;

(b) TLPT vodi organ za TLPT finančnega subjekta, določenega v skladu s točko (a), razen če se organi za TLPT finančnih subjektov, ki sodelujejo v skupinskem TLPT, dogovorijo drugače;

(c) organi za TLPT finančnih subjektov, ki niso finančni subjekt, določen za vodenje skupinskega TLPT, lahko bodisi izrazijo interes za spremljanje TLPT v vlogi opazovalcev bodisi imenujejo vodjo testiranja za ta TLPT.

Vodilni organ za TLPT usklajuje vse organe za TLPT, ki so vključeni v skupinski TLPT, ter sprejema vse odločitve, ki so potrebne za zanesljivo in učinkovito izvajanje skupinskega TLPT.

4. Kadar namerava finančni subjekt izvesti skupni TLPT iz člena 26(4) Uredbe (EU) 2022/2554, ki lahko vključuje finančne subjekte s sedežem v drugih državah članicah, njegov organ za TLPT stopi v stik z organi za TLPT drugih finančnih subjektov ter z njimi oceni izvedljivost in ustreznost izvajanja skupnega TLPT za te finančne subjekte v skladu s členom 26(4) Uredbe (EU) 2022/2554.

5. Za namene izvajanja skupnega TLPT iz člena 26(4) Uredbe (EU) 2022/2554:

(a) se organi za TLPT finančnih subjektov dogovorijo o tem, kateri finančni subjekt bo določen za izvajanje skupnega TLPT, ob upoštevanju storitev IKT, ki jih finančnim subjektom zagotavlja tretji ponudnik storitev IKT, in učinkovitosti testiranja;

(b) TLPT vodi organ za TLPT finančnega subjekta, določenega v skladu s točko (a), razen če se organi za TLPT finančnih subjektov, ki sodelujejo v skupnem TLPT, dogovorijo drugače;

(c) lahko organi za TLPT finančnih subjektov, ki niso finančni subjekt, določen za vodenje skupnega TLPT, bodisi izrazijo interes za spremljanje TLPT v vlogi opazovalcev bodisi imenujejo vodjo testiranja za ta TLPT.

Vodilni organ za TLPT usklajuje vse organe za TLPT, ki so vključeni v skupni TLPT, ter sprejema vse odločitve, ki so potrebne za zanesljivo in učinkovito izvajanje skupnega TLPT.

6. Kadar se organ za TLPT finančnega subjekta, ki mora izvajati TLPT, razlikuje od njegovega pristojnega organa iz člena 46 Uredbe (EU) 2022/2554, ta organa izmenjata vse relevantne informacije v zvezi z vsemi zadevami, povezanimi s TLPT, za namene izvajanja TLPT ali opravljanja svojih nalog v skladu z navedeno uredbo.

Člen 17

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 13. februarja 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

Vsebina projektne listine (člen 9(2), točka (a))

Informacija	Zahtevane informacije
Oseba, odgovorna za projektni načrt, tj. vodja nadzorne ekipe	Ime Kontaktni podatki
Preizkuševalci	☐ notranji ☐ zunanji ☐ oboji
Komunikacijski kanali, izbrani v skladu s členom 9(2), točka (d), in členom 9(4), točka (a), vključno s: (a) šifriranjem e-pošte, ki se uporablja; (b) spletnimi podatkovnimi sobami, ki se uporabljajo; (c) takojšnjim sporočanjem, ki se uporablja	
Šifra za TLPT	
Morebitne kritične ali pomembne funkcije, ki jih finančni subjekt opravlja v drugih državah članicah	1. Seznam kritičnih ali pomembnih funkcij, ki se opravljajo v drugi državi članici 2. Za vsako kritično ali pomembno funkcijo navedba države članice ali držav članic, v katerih se opravljajo
Morebitne kritične ali pomembne funkcije, ki jih podpirajo tretji ponudniki storitev IKT	3. Seznam kritičnih ali pomembnih funkcij, ki jih podpirajo tretji ponudniki storitev IKT 4. Za vsako funkcijo identifikacija tretjega ponudnika storitev IKT
Pričakovani roki za zaključek:	
(1) pripravljalne faze v skladu s členom 9	llll–mm–dd
(2) faze testiranja v skladu s členoma 10 in 11	llll–mm–dd
(3) zaključne faze v skladu s členom 12	llll–mm–dd
(4) sanacijskega načrta v skladu s členom 13	llll–mm–dd

PRILOGA II

Vsebina dokumenta s specifikacijo obsega (člen 9(6))

1. Dokument s specifikacijo obsega vsebuje seznam vseh kritičnih ali pomembnih funkcij, ki jih opredeli finančni subjekt.

2. Za vsako opredeljeno kritično ali pomembno funkcijo se vključijo naslednje informacije:
   (a) kadar kritična ali pomembna funkcija ni vključena v obseg TLPT, pojasnitev razlogov za njeno nevključitev;
   (b) kadar je kritična ali pomembna funkcija vključena v obseg TLPT:
      (i) pojasnitev razlogov za njeno vključitev;
      (ii) opredeljeni sistemi IKT, ki podpirajo to kritično ali pomembno funkcijo;
      (iii) za vsak opredeljeni sistem IKT:
         1. ali je oddan v zunanje izvajanje in če je, ime tretjega ponudnika storitev IKT;
         2. jurisdikcije, v katerih se sistem IKT uporablja;
         3. opis predhodnih oznak na visoki ravni, v katerem je navedeno, kateri varnostni vidik zaupnosti, celovitosti, avtentičnosti ali razpoložljivosti je zajet v vsaki oznaki.

PRILOGA III

Vsebina ciljno usmerjenega poročila o obveščevalnih podatkih o grožnjah (člen 10(5))

Ciljno usmerjeno poročilo o obveščevalnih podatkih o grožnjah vsebuje informacije, ki zajemajo vse naslednje:

1. splošni obseg raziskav na področju obveščevalnih podatkov, ki vključuje vsaj naslednje:
   (a) kritične ali pomembne funkcije, vključene v obseg;
   (b) njihovo geografsko lokacijo;
   (c) uradni jezik EU, ki se uporablja;
   (d) zadevne tretje ponudnike storitev IKT;
   (e) časovno obdobje, v katerem se zbirajo raziskave;
2. splošno oceno, katere konkretne obveščevalne podatke, na podlagi katerih je mogoče ukrepati, je mogoče najti o finančnem subjektu, med drugim:
   (a) uporabniška imena in gesla zaposlenih;
   (b) podobne domene, ki se lahko zmotno razumejo kot uradne domene finančnega subjekta;
   (c) tehnično izvidništvo: ranljiva programska oprema, sistemi in tehnologije ali programska oprema, sistemi in tehnologije, ki jih je mogoče izkoristiti;
   (d) informacije, ki jih zaposleni objavijo na internetu, povezane s finančnim subjektom, ki se lahko uporabijo za napad;
   (e) informacije, ki so naprodaj na temnem spletu;
   (f) kakršne koli druge pomembne informacije, ki so na voljo na internetu ali v javnih omrežjih;
   (g) kadar je ustrezno, fizično usmerjene informacije, vključno z načini dostopa do prostorov finančnega subjekta;
3. analizo obveščevalnih podatkov o grožnjah ob upoštevanju splošne krajine groženj in posebnega položaja finančnega subjekta, ki vključuje vsaj:
   (a) geopolitično okolje;
   (b) gospodarsko okolje;
   (c) tehnološke trende in vse druge trende, povezani z dejavnostmi v sektorju finančnih storitev;
4. profile groženj zlonamernih akterjev (določen posameznik/skupina ali generični razred), ki so lahko usmerjeni proti finančnemu subjektu, vključno s sistemi finančnega subjekta, ki bodo najverjetneje ogroženi ali bodo tarča zlonamernih akterjev, morebitno motivacijo, namero in utemeljitvijo morebitnega napadanja ter možnim načinom delovanja napadalcev;
5. scenarije groženj: vsaj tri celostne scenarije groženj za profile groženj, opredeljene v skladu s točko 4, ki imajo najvišje ocene resnosti grožnje. Scenariji groženj opisujejo celotno napadno pot in vključujejo vsaj:
   (a) en scenarij, ki med drugim vključuje ogroženo razpoložljivost storitev;
   (b) en scenarij, ki med drugim vključuje ogroženo celovitost podatkov;
   (c) en scenarij, ki med drugim vključuje ogroženo zaupnost informacij;
6. po potrebi opis scenarija, ki ne temelji na analizi groženj, iz člena 10(4).

PRILOGA IV

Vsebina načrta testiranja rdeče ekipe (člen 11(1))

Načrt testiranja rdeče ekipe vsebuje informacije, ki zajemajo vse naslednje:

(a) komunikacijske kanale in postopke;

(b) taktike, tehnike in postopke, ki so dovoljeni oziroma niso dovoljeni za uporabo v napadu, vključno z etičnimi omejitvami za socialni inženiring;

(c) ukrepe za obvladovanje tveganja, ki jih morajo upoštevati preizkuševalci;

(d) opis za vsak scenarij, ki vključuje:

  (i) simuliranega akterja grožnje;

  (ii) njegovo namero, motivacijo in cilje;

  (iii) ciljne funkcije in podporne sisteme IKT;

  (iv) ciljno usmerjene vidike zaupnosti, celovitosti, razpoložljivosti in avtentičnosti;

  (v) oznake;

(e) podroben opis vsake pričakovane napadne poti, vključno s predpogoji in možno pomočjo, ki jo mora zagotoviti nadzorna ekipa, vključno z roki za njeno zagotovitev in morebitno uporabo;

(f) načrtovanje dejavnosti testiranja rdeče ekipe, vključno s časovnim načrtovanjem za izvedbo vsakega scenarija, ki so razdeljene vsaj na tri faze, ki jih preizkuševalec izvede v celotni fazi testiranja, in sicer vstop v sisteme IKT finančnih subjektov, prehod prek sistemov IKT in končno izvajanje ukrepov v zvezi s cilji ter nazadnje umik iz sistemov IKT (faza vstopa, prehoda in izstopa);

(g) posebnosti infrastrukture finančnih subjektov, ki jih je treba upoštevati pri testiranju;

(h) morebitne dodatne informacije ali druge vire, ki jih preizkuševalci potrebujejo za izvedbo scenarijev.

PRILOGA V

Vsebina poročila o testiranju rdeče ekipe (člen 12(2))

Poročilo o testiranju rdeče ekipe vsebuje informacije, ki zajemajo vsaj vse naslednje:

(a) informacije o izvedenem napadu, ki vključujejo:

  (i) izbrane kritične ali pomembne funkcije ter opredeljene sisteme, postopke in tehnologije IKT, ki podpirajo kritično ali pomembno funkcijo, kot so opredeljeni v načrtu testiranja rdeče ekipe;

  (ii) povzetek vsakega scenarija;

  (iii) oznake, ki so bile oziroma niso bile dosežene;

  (iv) napadne poti, ki so jim uspešno oziroma neuspešno sledili;

  (v) uspešno oziroma neuspešno uporabljene taktike, tehnike in postopke;

  (vi) morebitna odstopanja od načrta testiranja rdeče ekipe;

  (vii) morebitno ponujeno pomoč;

(b) vse ukrepe, za katere preizkuševalci vedo, da jih je izvedla modra ekipa, da bi rekonstruirala napad in zmanjšala njegove učinke;

(c) odkrite ranljivosti in druge ugotovitve, ki vključujejo:

  (i) opis ranljivosti in drugih ugotovitev, vključno z njihovo kritičnostjo;

  (ii) analizo temeljnih vzrokov uspešnih napadov;

  (iii) priporočila za sanacijo, vključno z navedbo pomembnosti sanacije.

PRILOGA VI

Vsebina poročila o testiranju modre ekipe (člen 12(4))

Poročilo o testiranju modre ekipe vsebuje informacije, ki zajemajo vsaj vse naslednje:

1. za vsako fazo napada, ki so jo opisali preizkuševalci v poročilu o testiranju rdeče ekipe:
   (a) seznam odkritih dejanj napada;
   (b) dnevniške vnose, ki ustrezajo tem odkritjem;
2. oceno ugotovitev in priporočil preizkuševalcev;
3. dokaze o napadu preizkuševalcev, ki jih je zbrala modra ekipa;
4. analizo temeljnih vzrokov uspešnih napadov preizkuševalcev, ki jo je opravila modra ekipa;
5. seznam pridobljenih izkušenj in ugotovljenih možnosti za izboljšave;
6. seznam tem, ki jih je treba obravnavati v povezovanju v vijolično ekipo.

PRILOGA VII

Podrobnosti poročila s povzetkom relevantnih ugotovitev TLPT iz člena 26(6) Uredbe (EU) 2022/2554

Zbirno poročilo o testiranju vsebuje informacije, ki zajemajo vsaj vse naslednje:

(a) sodelujoče stranke;

(b) projektni načrt;

(c) potrjeni obseg, vključno z utemeljitvijo vključitve ali izključitve kritičnih ali pomembnih funkcij ter opredeljenih sistemov, postopkov in tehnologij IKT, ki podpirajo kritične ali pomembne funkcije, zajete v TLPT;

(d) izbrane scenarije in morebitna znatna odstopanja od ciljno usmerjenega poročila o obveščevalnih podatkih o grožnjah;

(e) izvedene napadne poti ter uporabljene taktike, tehnike in postopki;

(f) zajete in nezajete oznake;

(g) morebitna odstopanja od načrta testiranja rdeče ekipe;

(h) morebitna odkritja modre ekipe;

(i) povezovanje v vijolično ekipo v fazi testiranja, če se izvaja, in povezane pogoje;

(j) morebitno uporabljeno pomoč;

(k) sprejete ukrepe za obvladovanje tveganja;

(l) ugotovljene ranljivosti in druge ugotovitve, vključno z njihovo kritičnostjo;

(m) analizo temeljnih vzrokov uspešnih napadov;

(n) načrt na visoki ravni za sanacijo, ki povezuje ranljivosti in druge ugotovitve, njihove temeljne vzroke in pomembnost sanacije;

(o) spoznanja, pridobljena na podlagi prejetih povratnih informacij.

PRILOGA VIII

Podrobnosti potrdila o TLPT iz člena 26(7) Uredbe (EU) 2022/2554

Potrdilo vsebuje vsaj vse naslednje informacije:

(a) o izvedenem TLPT:

(i) začetni in končni datum TLPT;

(ii) kritične ali pomembne funkcije, vključene v obseg testiranja;

(iii) kadar je ustrezno, informacije o kritičnih ali pomembnih funkcijah, vključenih v obseg testiranja, v zvezi s katerimi TLPT ni bil izveden;

(iv) kadar je ustrezno, druge finančne subjekte, ki so bili vključeni v TLPT;

(v) kadar je ustrezno, tretje ponudnike storitev IKT, ki so sodelovali pri TLPT;

(vi) v zvezi s preizkuševalci:

1. ali so bili uporabljeni notranji preizkuševalci;

2. ali je finančni subjekt uporabil člen 5(3), drugi pododstavek;

(vii) trajanje faze aktivnega testiranja rdeče ekipe v koledarskih dneh;

(b) če je bilo v TLPT vključenih več organov za TLPT, druge organe za TLPT in njihovo vlogo;

(c) seznam dokumentov, ki jih je organ za TLPT pregledal za namene potrdila.