2025/1190

18.6.2025

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2025/1190

ze dne 13. února 2025,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující kritéria, která se použijí pro určení finančních subjektů, které jsou povinny provádět penetrační testování na základě hrozeb, požadavky a normy, kterými se řídí využívání interních subjektů provádějících testování, požadavky týkající se rozsahu testování, metodiky a postupů testování pro jednotlivé fáze procesu testování, výsledků a fáze ukončení testování a nápravy a druhu spolupráce v oblasti dohledu a jiné relevantní spolupráce, která je zapotřebí k provádění penetračního testování na základě hrozeb a pro usnadnění vzájemného uznávání těchto testů

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského Parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 ([1]), a zejména na čl. 26 odst. 11 čtvrtý pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Toto nařízení bylo vypracováno v souladu s rámcem TIBER-EU a odráží metodiku, proces a strukturu penetračního testování na základě hrozeb, jak je popsáno v rámci TIBER-EU. Finanční subjekty, na které se vztahuje penetrační testování na základě hrozeb, mohou odkazovat na rámec TIBER-EU nebo na některé jeho vnitrostátní prováděcí opatření a uplatňovat je, pokud je tento rámec nebo toto vnitrostátní prováděcí opatření v souladu s požadavky stanovenými v článcích 26 a 27 nařízení (EU) 2022/2554 a v tomto nařízení. Určením jediného veřejného orgánu ve finančním sektoru, který bude na vnitrostátní úrovni odpovědný za záležitosti související s penetračním testováním na základě hrozeb v souladu s čl. 26 odst. 9 nařízení (EU) 2022/2554, by neměla být dotčena pravomoc příslušných orgánů svěřená na úrovni Unie pro dohled nad některými finančními subjekty v souladu s článkem 46 uvedeného nařízení, jakou je například pravomoc svěřená Evropské centrální bance příslušné k provádění dohledu nad významnými úvěrovými institucemi, které mají být považovány za příslušné pro záležitosti týkající se penetračního testování na základě hrozeb. Pokud je podle čl. 26 odst. 10 nařízení (EU) 2022/2554 jiný vnitrostátní orgán ve finančním sektoru pověřen výkonem pouze některých úkolů souvisejících s penetračním testováním na základě hrozeb, měl by příslušným orgánem pro úkoly související s penetračním testováním na základě hrozeb, jejichž výkonem nebyl pověřen žádný jiný orgán, zůstat příslušný orgán finančního subjektu uvedený v článku 46 uvedeného nařízení.

(2) Vzhledem ke složitosti penetračního testování na základě hrozeb a rizikům s ním spojeným by se jeho použití mělo omezit na ty finanční subjekty, u nichž je to odůvodněné. Proto by orgány odpovědné za záležitosti související s penetračním testováním na základě hrozeb (orgány pro penetrační testování na základě hrozeb buď na úrovni Unie, nebo na vnitrostátní úrovni) měly z rozsahu penetračního testování na základě hrozeb vyloučit ty finanční subjekty, které působí v hlavních pododvětvích finančních služeb, pro něž není penetrační testování na základě hrozeb odůvodněné. To znamená, že od požadavku na penetrační testování na základě hrozeb by mohly být osvobozeny úvěrové instituce, platební instituce a instituce elektronických peněz, centrální depozitáře cenných papírů, ústřední protistrany, obchodní systémy, pojišťovny a zajišťovny, přestože splňují kvantitativní kritéria, a to s ohledem na celkové posouzení jejich rizikového profilu a vyspělosti v oblasti IKT, dopadu na finanční sektor a souvisejících hledisek finanční stability.

(3) Orgány pro penetrační testování na základě hrozeb by měly s ohledem na celkové posouzení rizikového profilu a vyspělosti v oblasti IKT, dopadu na finanční sektor a souvisejících hledisek finanční stability posoudit, zda by se penetrační testování na základě hrozeb mělo vztahovat na jakýkoli typ finančního subjektu kromě úvěrových institucí, platebních institucí, institucí elektronických peněz, ústředních protistran, centrálních depozitářů cenných papírů, obchodních systémů, pojišťoven a zajišťoven. Posouzení, zda tyto finanční subjekty splňují tato kvalitativní kritéria, by mělo být zaměřeno na určení finančních subjektů, pro které je penetrační testování na základě hrozeb vhodné, a to pomocí meziodvětvových a objektivních ukazatelů. Zároveň by se posuzování, zda finanční subjekt splňuje tato kvalitativní kritéria, mělo omezit na ty dotčené subjekty, u nichž je toto penetrační testování na základě

([1]) Úř. věst. L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

hrozeb odůvodněné. To, zda finanční subjekt splňuje tato kvalitativní kritéria, by mělo být posuzováno také s ohledem na vývoj nových trhů a na rostoucí význam nových účastníků trhu pro finanční sektor v budoucnu, včetně poskytovatelů služeb souvisejících s kryptoaktivy povolených v souladu s článkem 59 nařízení Evropského parlamentu a Rady (EU) 2023/1114 ([2]).

(4) Finanční subjekty mohou mít stejného poskytovatele služeb IKT v rámci skupiny nebo mohou patřit do stejné skupiny a spoléhat se na využívání sdílených systémů IKT. V takovém případě je důležité, aby orgány pro penetrační testování na základě hrozeb při posuzování toho, zda by se na finanční subjekt mělo vztahovat penetrační testování na základě hrozeb a zda by penetrační testování na základě hrozeb mělo být prováděno na úrovni subjektu nebo na úrovni skupiny (prostřednictvím sdruženého penetrační testování na základě hrozeb), zvážily strukturu a systémovou povahu nebo význam tohoto finančního subjektu pro finanční sektor na vnitrostátní úrovni nebo na úrovni Unie.

(5) Aby metodika testování odrážela rámec TIBER-EU, je nutné, aby umožňovala zapojení těchto hlavních účastníků: finančního subjektu s řídícím týmem (odrážejícího „řídící tým“ rámce TIBER-EU) a modrým týmem (odrážejícím „modrý tým“ rámce TIBER-EU) a orgánu pro penetrační testování na základě hrozeb v podobě kybernetického týmu pro penetrační testování na základě hrozeb (odrážejícího „kybernetické týmy“ rámce TIBER-EU), poskytovatele operativních informací o hrozbách a subjektů provádějících testování (přičemž subjekty provádějící testování odrážejí „červený tým“ rámce TIBER-EU).

(6) Aby se zajistilo, že penetrační testování na základě hrozeb bude těžit ze zkušeností získaných při provádění rámce TIBER-EU, a aby se snížila rizika spojená s prováděním penetračního testování na základě hrozeb, mělo by se zajistit, že povinnosti kybernetických týmů pro penetrační testování na základě hrozeb, které mají být zřízeny na úrovni orgánů pro penetrační testování na základě hrozeb, budou co nejvíce odpovídat povinnostem kybernetických týmů rámce TIBER-EU. Proto by kybernetické týmy pro penetrační testování na základě hrozeb měly mít vedoucí pracovníky pro testy, kteří budou odpovědní za dohled nad jednotlivými testy v rámci penetračního testování na základě hrozeb a za plánování a koordinaci jednotlivých testů. Kybernetické týmy pro penetrační testování na základě hrozeb by měly sloužit jako jediné kontaktní místo pro komunikaci s interními a externími zúčastněnými stranami ohledně testování, pro shromažďování a zpracovávání zpětné vazby a zkušeností z dříve provedených testů a pro podporu finančních subjektů, které penetrační testování na základě hrozeb podstupují.

(7) Aby byla zohledněna metodika rámce TIBER-EU, měli by mít vedoucí pracovníci pro testy dovednosti a schopnosti potřebné k poskytování poradenství a ověřování návrhů subjektů provádějících testování. Zkušenosti s rámcem TIBER-EU ukázaly, že je přínosné mít ke každému testu přidělen tým zahrnující alespoň dva vedoucí pracovníky pro testy. S ohledem na to, že penetrační testování na základě hrozeb slouží k podpoře získávání zkušeností, se orgánům pro penetrační testování na základě hrozeb z důvodu ochrany důvěrnosti testů, a pokud nemají problémy se zdroji nebo odbornými znalostmi, důrazně doporučuje, aby vzaly na vědomí, že po dobu trvání penetračního testování na základě hrozeb by vedoucí pracovníci pro testy neměli provádět činnosti dohledu nad stejným finančním subjektem, který prochází penetračním testováním na základě hrozeb.

(8) Pro zajištění souladu s rámcem TIBER-EU je důležité, aby orgán pro penetrační testování na základě hrozeb pečlivě sledoval testování v každé jeho fázi. Vzhledem k povaze testování a rizikům s ním spojeným je zásadní, aby byl orgán pro penetrační testování na základě hrozeb zapojen do každé konkrétní fáze testování. Orgán pro penetrační testování na základě hrozeb by měl být zejména konzultován a měl by potvrdit posouzení nebo rozhodnutí finančních subjektů, která mohou na jedné straně ovlivnit účinnost testu a na druhé straně mít dopad na rizika spojená s testem. K základním krokům, do nichž se musí orgán pro penetrační testování na základě hrozeb konkrétně zapojit, patří potvrzování určité základní dokumentace testování a výběr poskytovatelů operativních informací o hrozbách a subjektů provádějících testování a opatření k řízení rizik. Zapojení orgánů pro penetrační testování na základě hrozeb, zejména do potvrzování, by nemělo vést k nadměrné zátěži těchto orgánů, a mělo by se proto omezit na dokumenty a rozhodnutí, které přímo ovlivňují provádění penetračního testování na základě hrozeb. Díky aktivní účasti v každé fázi testování mohou orgány pro penetrační testování na základě hrozeb účinně posoudit soulad finančních subjektů s příslušnými požadavky, což by mělo těmto orgánům umožnit vydávat osvědčení podle čl. 26 odst. 7 nařízení (EU) 2022/2554.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 (Úř. věst. L 150, 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Důvěrný charakter penetračního testování na základě hrozeb má zásadní význam pro zajištění reálných podmínek testování. Z tohoto důvodu by mělo být testování skryté, měla by být přijata opatření k zachování důvěrnosti penetračního testování na základě hrozeb a měly by být mimo jiné vybrány názvy kódů, které by měly být navrženy tak, aby třetím stranám zabránily zjištění penetračního testování na základě hrozeb. Pokud by se zaměstnanci odpovědní za bezpečnost finančního týmu dozvěděli o plánovaném nebo probíhajícím penetračním testování na základě hrozeb, je pravděpodobné, že by byli pozornější a ostražitější než za běžných pracovních podmínek, což by vedlo ke změně výsledku testování. Zaměstnanci finančního subjektu mimo řídící tým by proto měli být o plánovaném nebo probíhajícím penetračním testování na základě hrozeb informováni pouze v případě, že k tomu existují pádné důvody, a po předchozím souhlasu vedoucích pracovníků pro testy, mimo jiné proto, aby byla zajištěna důvěrnost testu pro případ, že by člen modrého týmu testování odhalil.

(10) Jak vyplývá ze zkušeností získaných rámcem TIBER-EU v souvislosti s „řídícím týmem“, je pro bezpečné provádění penetračního testování na základě hrozeb nezbytný výběr vhodného vedoucího člena řídícího týmu. Vedoucí člen řídícího týmu by měl mít v rámci finančního subjektu potřebný mandát k řízení všech aspektů testování, aniž by byla narušena jeho důvěrnost. Ze stejného důvodu by členové řídícího týmu měli mít hluboké znalosti o finančním subjektu, o pracovní roli vedoucího člena řídícího týmu a o jeho strategickém postavení, měli by mít požadovanou délku výkonu funkce a přístup ke správní radě. Aby se snížilo riziko narušení penetračního testování na základě hrozeb, měl by být řídící tým co nejmenší.

(11) S penetračním testováním na základě hrozeb jsou neodmyslitelně spojena rizika, protože zásadní funkce jsou testovány v produkčním prostředí za provozu, což může způsobit incidenty odmítnutí služby, neočekávané pády systému, poškození kritických produkčních systémů za provozu nebo ztrátu, modifikaci či zveřejnění dat. Tato rizika zdůrazňují potřebu důkladných opatření k řízení rizik. Aby bylo zajištěno, že penetrační testování na základě hrozeb bude po celou dobu testování probíhat kontrolovaně, je velmi důležité, aby si finanční subjekty byly ve všech bodech vědomy konkrétních rizik, která při penetračním testování na základě hrozeb vznikají, a aby tato rizika byla zmírněna. V tomto ohledu, aniž by byly dotčeny interní procesy finančního subjektu a odpovědnost a pověření, které již byly svěřeny vedoucímu členovi řídícího týmu, může být vhodné poskytnout informace o opatřeních k řízení rizik v souvislosti s penetračním testováním na základě hrozeb nebo v konkrétních případech může být vhodné schválení těchto opatření k řízení rizik samotným vedoucím orgánem finančního subjektu. Aby bylo možné poskytovat efektivní a co nejkvalifikovanější odborné služby a snižovat tato rizika, je také nezbytné, aby subjekty provádějící testování a poskytovatelé operativních informací o hrozbách (společně poskytovatelé penetračního testování na základě hrozeb) měli nejvyšší úroveň dovedností, odborných znalostí a odpovídající zkušenosti v oblasti operativních informací o hrozbách a penetračního testování na základě hrozeb v odvětví finančních služeb.

(12) Běžné penetrační testy poskytují podrobné a užitečné posouzení technických a konfiguračních zranitelností často jednoho izolovaného systému nebo prostředí, ale na rozdíl od na operativních informacích založeného (metoda „červeného týmu“) testování nehodnotí celý scénář cíleného útoku na celý subjekt, ani kompletní rozsah jeho lidského kapitálu, procesů a technologií. Finanční subjekty by se proto měly při výběru poskytovatelů penetračního testování na základě hrozeb ujistit, že tito poskytovatelé mají potřebné dovednosti k provádění na operativních informacích založeného (metoda „červeného týmu“) testování, a nikoli pouze penetračních testů. Je proto nutné stanovit komplexní kritéria pro interní i externí subjekty provádějící testování a poskytovatele operativních informací o hrozbách, vždy externí. Pokud poskytovatelé penetračního testování na základě hrozeb patří do stejné společnosti, měli by být zaměstnanci pověření penetračním testováním na základě hrozeb náležitě odděleni.

(13) Mohou nastat výjimečné okolnosti, za kterých finanční subjekty nemohou uzavřít smlouvu s poskytovateli penetračního testování na základě hrozeb, kteří splňují komplexní kritéria. Finanční subjekty by proto měly mít po prokázání nedostupnosti těchto poskytovatelů operativních informací o hrozbách možnost zapojit osoby, které nesplňují všechna komplexní kritéria, za předpokladu, že řádně zmírní veškerá z toho vyplývající dodatečná rizika a že orgán pro penetrační testování na základě hrozeb všechna tato kritéria posoudí.

(14) Pokud se na penetračním testování na základě hrozeb podílí několik finančních subjektů a několik orgánů pro penetrační testování na základě hrozeb, měly by být v procesu penetračního testování na základě hrozeb upřesněny role všech stran, aby bylo možné provést co nejefektivnější a nejbezpečnější test. Pro účely společného testování je nutné stanovit zvláštní požadavky na úlohu určeného finančního subjektu, konkrétně to, že by měl být odpovědný za poskytování veškeré potřebné dokumentace vedoucímu orgánu pro penetrační testování na základě hrozeb a za monitorování procesu testování. Určený finanční subjekt by měl mít na starosti také společné aspekty hodnocení řízení rizik. Bez ohledu na roli určeného finančního subjektu by neměly být během společného testu dotčeny povinnosti jednotlivých finančních subjektů, které se účastní procesu společného penetračního testování na základě hrozeb. Stejná zásada by měla platit i pro sdružené penetrační testování na základě hrozeb.

(15) Jak ukazují zkušenosti s prováděním rámce TIBER-EU, nejefektivnějším způsobem, jak zajistit řádný průběh testování, je pořádání osobních nebo virtuálních schůzek zahrnujících všechny zúčastněné strany (finanční subjekty, orgány, subjekty provádějící testování a poskytovatele operativních informací o hrozbách). Osobní a virtuální schůzky by se proto měly konat v různých fázích procesu, a to zejména ve fázi přípravy a při zahájení penetračního testování na základě hrozeb za účelem dokončení vymezení jeho rozsahu, ve fázi testování za účelem dokončení zprávy o operativních informacích o hrozbách a plánu testování metodou „červeného týmu“ a za účelem týdenních aktualizací a ve fázi ukončení k zopakování akcí subjektů provádějících testování a modrého týmu, testování metodou „fialového týmu“ a za účelem výměny zpětné vazby k penetračnímu testování na základě hrozeb.

(16) Aby bylo zajištěno bezproblémové provádění penetračního testování na základě hrozeb, měl by orgán pro penetrační testování na základě hrozeb finančnímu subjektu jasně sdělit svá očekávání ohledně testování. V tomto ohledu by měli vedoucí pracovníci pro testy zajistit, aby byl vytvořen vhodný tok informací s řídícím týmem v rámci finančního subjektu a s poskytovateli penetračního testování na základě hrozeb.

(17) Finanční subjekt by měl vybrat zásadní nebo důležité funkce, které budou spadat do rozsahu penetračního testování na základě hrozeb. Při výběru těchto funkcí by měl finanční subjekt vycházet z různých kritérií týkajících se významu každé funkce pro samotný finanční subjekt a pro finanční sektor na úrovni Unie a na vnitrostátní úrovni, a to nejen z ekonomického hlediska, ale také s ohledem na symbolický nebo politický status funkce. Pro usnadnění bezproblémového přechodu do fáze shromažďování operativních informací o hrozbách by měl řídící tým poskytnout subjektům provádějícím testování a poskytovatelům operativních informací o hrozbách, kteří nejsou zapojeni do procesu stanovení rozsahu, podrobné informace o dohodnutém rozsahu.

(18) Aby subjektům provádějícím testování poskytl informace potřebné k simulaci skutečného a realistického útoku na systémy finančního subjektu za provozu, které jsou základem jeho zásadních nebo důležitých funkcí, měl by poskytovatel operativních informací o hrozbách shromažďovat operativní informace nebo informace, které pokrývají alespoň dvě klíčové oblasti zájmu: cíle, a to identifikací potenciálních prostorů k útoku v rámci finančního subjektu, a hrozby, a to identifikací příslušných aktérů hrozeb a pravděpodobných scénářů hrozeb. Aby se zajistilo, že poskytovatel operativních informací o hrozbách zohlední relevantní hrozby pro finanční subjekt, měly by subjekty provádějící testování, řídící tým a vedoucí pracovníci pro testy poskytnout zpětnou vazbu k návrhu zprávy o operativních informacích o hrozbách. Pokud je k dispozici, může poskytovatel operativních informací o hrozbách použít jako základ pro vnitrostátní prostředí hrozeb generické prostředí hrozeb poskytnuté orgánem pro penetrační testování na základě hrozeb pro finanční sektor členského státu. Na základě uplatňování rámce TIBER-EU trvá proces shromažďování operativních informací o hrozbách obvykle přibližně čtyři týdny.

(19) Aby mohly subjekty provádějící testování získat přehled a podrobněji přezkoumat dokument upřesňující rozsah a zprávu o cílených operativních informacích o hrozbách, a dokončit tak plán testování metodou „červeného týmu“, je nezbytné, aby před fází testování metodou „červeného týmu“ v rámci penetračního testování na základě hrozeb obdržely od poskytovatele operativních informací o hrozbách podrobné vysvětlení zprávy o cílených operativních informacích o hrozbách a analýzu možných scénářů hrozeb.

(20) Aby mohly subjekty provádějící testování provést realistické a komplexní testování, při kterém se provedou všechny fáze útoku a dosáhne se příznaků, měla by být na fázi aktivního testování metodou „červeného týmu“ vyhrazena dostatečná doba. Na základě zkušeností získaných s rámcem TIBER-EU by měla být vyhrazená doba dlouhá nejméně dvanáct týdnů a měla by být stanovena s ohledem na počet zúčastněných stran, rozsah penetračního testování na základě hrozeb, zdroje zúčastněného finančního subjektu nebo zúčastněných finančních subjektů, případné externí požadavky a dostupnost podpůrných informací poskytnutých finančním subjektem.

(21) Ve fázi aktivního testování metodou „červeného týmu“ by měly subjekty provádějící testování využívat řadu taktik, technik a postupů, aby adekvátně otestovaly produkční systémy finančního subjektu za provozu. Taktiky, techniky a postupy by měly podle potřeby zahrnovat průzkum (tj. shromáždění co největšího množství informací o cíli), přípravu (tj. analýzu informací o infrastruktuře, zařízeních a zaměstnancích a přípravu na operace specifické pro daný cíl), spuštění (tj. aktivní zahájení kompletní operace zaměřené na cíl), využití (tj. kdy je cílem subjektů provádějících testování kompromitovat servery, sítě finančního subjektu a využít jeho zaměstnance prostřednictvím sociálního inženýrství), kontrolu a přesun (tj. pokusy o přesun z kompromitovaných systémů do dalších zranitelných systémů nebo systémů s vysokou hodnotou) a opatření zaměřená na cíl (tj. získání širšího přístupu do kompromitovaných systémů a získání přístupu k předem dohodnutým informacím a datům cíle, jak bylo předem dohodnuto v plánu testování metodou „červeného týmu“).

(22) Při provádění penetračního testování na základě hrozeb by měly subjekty provádějící testování postupovat s ohledem na dobu, která je k provedení útoku k dispozici, zdroje a etické a právní hranice. Pokud by subjekty provádějící testování nedokázaly postoupit do další naprogramované fáze útoku, měl by jim řídící tým po dohodě s orgánem pro penetrační testování na základě hrozeb poskytnout příležitostnou pomoc ve formě „podpory“. Podporu lze obecně rozdělit na informační a přístupovou; může spočívat v poskytnutí přístupu do systémů IKT nebo interních sítí, aby bylo možné pokračovat v testu a zaměřit se na následující kroky útoku.

(23) Během aktivního testování nasazením „červeného týmu“ ve fázi testování by mělo být využito společné testování, do kterého se zapojí jak subjekty provádějící testování, tak modrý tým, pokud je to nutné, aby bylo možné pokračovat v penetračním testování na základě hrozeb jako poslední možnosti za výjimečných okolností a po vyčerpání všech alternativních možností. V rámci tohoto omezeného testování metodou „fialového týmu“ lze použít následující metody: metodu „catch-and-release“, kdy se subjekty provádějící testování pokoušejí pokračovat ve scénářích, jsou odhaleni a poté pokračují v testování, metodu „war gaming“, která umožňuje složitější scénáře pro testování strategického rozhodování, nebo metodu „collaborative proof-of-concept“, která umožňuje subjektům provádějící testování a členům modrého týmu společně ověřovat konkrétní bezpečnostní opatření, nástroje nebo techniky v kontrolovaném a spolupracujícím prostředí.

(24) Penetrační testování na základě hrozeb by mělo sloužit k získávání zkušeností s cílem zvýšit digitální provozní odolnost finančních subjektů. V tomto ohledu by modrý tým a subjekty provádějící testování měly útok zopakovat a ve spolupráci se subjekty provádějícími testování přezkoumat kroky, které byly podniknuty, aby se z testování poučily. Za tímto účelem a s cílem umožnit odpovídající přípravu by měly být zpráva o testování metodou „červeného týmu“ a zpráva o testování metodou „modrého týmu“ zpřístupněny všem stranám zapojeným do zopakování před tím, než budou provedeny jakékoli činnosti v rámci zopakování. Ve fázi ukončení by navíc mělo být provedeno testování metodou „fialového týmu“, aby se maximalizovaly získané zkušenosti. Metody, které mohou být použity pro testování metodou „fialového týmu“ ve fázi ukončení, by měly zahrnovat diskuse o alternativních scénářích útoku, zkoumání alternativních scénářů na systémech za provozu nebo opětovné zkoumání plánovaných scénářů na systémech za provozu, které se subjektům provádějícím testování nepodařilo dokončit nebo provést během fáze testování.

(25) Aby se zajistilo, že všechny zúčastněné strany zapojené do penetračního testování na základě hrozeb získají zkušenosti, aby se zlepšily budoucí testy a aby se posílila digitální provozní odolnost finančních subjektů, měly by si zúčastněné strany vzájemně poskytovat zpětnou vazbu k celému procesu a zejména určit, které činnosti probíhaly dobře nebo mohly být zlepšeny a které aspekty procesu penetračního testování na základě hrozeb fungovaly dobře nebo by mohly být zlepšeny.

(26) Příslušné orgány uvedené v článku 46 nařízení (EU) 2022/2554 a orgány pro penetrační testování na základě hrozeb by měly, pokud se liší, spolupracovat na začlenění pokročilého testování prostřednictvím penetračního testování na základě hrozeb do stávajících postupů dohledu. V tomto ohledu a za účelem zajištění správného pochopení zjištění z penetračního testování na základě hrozeb a jejich výkladu je vhodné, aby zejména v případě souhrnné zprávy o testu a plánů nápravných opatření byla navázána úzká spolupráce mezi vedoucími pracovníky pro testy, kteří se podíleli na penetračním testování na základě hrozeb, a odpovědnými orgány dohledu.

(27) Ustanovení čl. 26 odst. 8 prvního pododstavce nařízení (EU) 2022/2554 stanoví, že finanční subjekty musí provedení vždy jednoho ze tří testů zadat externímu subjektu provádějícímu testování. Pokud finanční subjekty zahrnují do týmu subjektů provádějících testování jak interní, tak externí subjekty provádějící testování, mělo by se pro účely uvedeného článku považovat penetrační testování na základě hrozeb za takové, jež je prováděné interními subjekty provádějícími testování.

(28) Toto nařízení je založeno na návrhu regulačních technických norem předloženém Komisi Evropským orgánem pro bankovnictví, Evropským orgánem pro pojišťovnictví a zaměstnanecké penzijní pojištění a Evropským orgánem pro cenné papíry a trhy (dále jen „evropské orgány dohledu“), a to po dohodě s Evropskou centrální bankou.

(29) Evropské orgány dohledu uspořádaly otevřené veřejné konzultace o návrzích regulačních technických norem, z nichž toto nařízení vychází, provedly analýzu potenciálních souvisejících nákladů a přínosů a vyžádaly si stanovisko skupiny subjektů působících v bankovnictví zřízené na základě článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([3]), skupiny subjektů působících v oblasti pojištění a zajištění a skupiny subjektů působících v oblasti zaměstnaneckého penzijního pojištění zřízených na základě článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ([4]) a skupiny subjektů působících v oblasti cenných papírů a trhů zřízené na základě článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ([5]).

(30) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([6]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 20. srpna 2024,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Definice

Pro účely tohoto nařízení se rozumí:

1) „řídícím týmem“ tým složený ze zaměstnanců testovaného finančního subjektu, a pokud je to s ohledem na rozsah penetračního testování na základě hrozeb relevantní, ze zaměstnanců jeho poskytovatelů služeb z řad třetích stran a jakékoli další zúčastněné strany, která řídí test;

2) „vedoucím členem řídícího týmu“ zaměstnanec finančního subjektu odpovědný za provádění všech činností souvisejících s penetračním testováním na základě hrozeb pro finanční subjekt v rámci daného testu;

3) „modrým týmem“ zaměstnanci finančního subjektu a případně zaměstnanci jeho poskytovatelů služeb z řad třetích stran a jakákoli další zúčastněná strana, která je považována za relevantní s ohledem na rozsah penetračního testování na základě hrozeb, jeho poskytovatelů služeb z řad třetích stran, kteří brání používání sítě a informačních systémů finančního subjektu tím, že udržují jeho stav zabezpečení před simulovanými nebo skutečnými útoky, a kteří si nejsou penetračního testování na základě hrozeb vědomi;

4) „úkoly modrého týmu“ úkoly, které obvykle vykonává modrý tým, jako jsou bezpečnostní operační středisko, služby infrastruktury IKT, služby helpdesku, služby řízení incidentů na provozní úrovni;

5) „červeným týmem“ interní nebo externí subjekty provádějící testování, které jsou pro penetrační testování na základě hrozeb najati nebo přiděleni;

6) „testováním metodou ‚fialového týmu‘“ společné testování, do kterého jsou zapojeny subjekty provádějící testování i modrý tým;

([3]) Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/79/ES (Úř. věst. L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/77/ES (Úř. věst. L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) „orgánem pro penetrační testování na základě hrozeb“:

   a) jediný veřejný orgán ve finančním sektoru určený v souladu s čl. 26 odst. 9 nařízení (EU) 2022/2554;

   b) orgán ve finančním sektoru, na který je delegován výkon některých nebo všech úkolů v souvislosti s penetračním testováním na základě hrozeb v souladu s čl. 26 odst. 10 nařízení (EU) 2022/2554;

   c) jakýkoli příslušný orgán uvedený v článku 46 nařízení (EU) 2022/2554;

8) „kybernetickým týmem pro penetrační testování na základě hrozeb“ zaměstnanci orgánů pro penetrační testování na základě hrozeb, kteří jsou odpovědní za záležitosti týkající se tohoto testování;

9) „vedoucími pracovníky pro testy“ zaměstnanci určení k vedení činností orgánu pro penetrační testování na základě hrozeb pro konkrétní penetrační testování na základě hrozeb za účelem sledování dodržování tohoto nařízení;

10) „poskytovatelem operativních informací o hrozbách“ odborníci najatí finančním subjektem pro každé penetrační testování na základě hrozeb, kteří jsou externí vůči finančnímu subjektu a případným poskytovatelům služeb IKT v rámci skupiny a kteří shromažďují a analyzují cílené operativní informace o hrozbách relevantní pro finanční subjekty v rámci konkrétního penetračního testování na základě hrozeb a vypracovávají odpovídající relevantní a realistické scénáře hrozeb;

11) „poskytovateli penetračního testování na základě hrozeb“ subjekty provádějící testování a poskytovatelé operativních informací o hrozbách;

12) „podporou“ pomoc nebo informace, které řídící tým poskytuje subjektům provádějícím testování, aby jim umožnil pokračovat v provádění cesty útoku, pokud nejsou schopni postupovat dále samy a pokud neexistuje jiná rozumná alternativa, a to i z důvodu nedostatečného času nebo zdrojů v daném penetračním testování na základě hrozeb;

13) „cestou útoku“ trasa, po které se subjekty provádějící testování během fáze aktivního testování metodou „červeného týmu“ v rámci penetračního testování na základě hrozeb dostanou k příznakům určeným pro dané penetrační testování na základě hrozeb;

14) „příznaky“ klíčové cíle v systémech IKT podporujících zásadní nebo důležité funkce finančního subjektu, kterých se subjekty provádějící testování snaží dosáhnout prostřednictvím testu;

15) „citlivými informacemi“ informace, které lze snadno využít k útokům na systémy IKT finančního subjektu, duševní vlastnictví, důvěrné obchodní údaje nebo osobní údaje, které mohou přímo či nepřímo poškodit finanční subjekt a jeho ekosystém, pokud by se dostaly do rukou zlovolných aktérů;

16) „skupinou“ všechny finanční subjekty, které se účastní společného penetračního testování na základě hrozeb podle čl. 26 odst. 4 nařízení (EU) 2022/2554;

17) „hostitelským členským státem“ hostitelský členský stát v souladu s odvětvovým právem Unie, které se vztahuje na každý finanční subjekt;

18) „sdruženým penetračním testováním na základě hrozeb“ se rozumí penetrační testování na základě hrozeb jiné než společné penetrační testování na základě hrozeb uvedené v čl. 26 odst. 4 nařízení (EU) 2022/2554, které zahrnuje několik finančních subjektů využívajících stejného poskytovatele služeb IKT v rámci skupiny nebo patřících do stejné skupiny a sdílejících systémy IKT.

Článek 2

Určení finančních subjektů, které jsou povinny provádět penetrační testování na základě hrozeb

1. Orgány pro penetrační testování na základě hrozeb posoudí, zda je některý finanční subjekt povinen provést penetrační testování na základě hrozeb, přičemž zohlední dopad těchto finančních subjektů, jejich systémovou povahu a jejich rizikový profil v oblasti IKT, a to na základě všech těchto kritérií:

a) faktorů souvisejících s dopady a systémovou povahou:

   i) velikosti finančního subjektu, která se určí na základě toho, zda finanční subjekt poskytuje finanční služby v jednom nebo více členských státech, a porovnáním činností finančního subjektu s činnostmi jiných finančních subjektů poskytujících podobné služby;

   ii) rozsahu a povahy propojení finančního subjektu s jinými finančními subjekty ve finančním sektoru v jednom nebo více členských státech;

   iii) významu nebo důležitosti služeb, které finanční subjekt poskytuje finančnímu sektoru;

iv) nahraditelnosti služeb, které finanční subjekt poskytuje;

v) složitosti obchodního modelu finančního subjektu a souvisejících služeb a procesů;

vi) zda je finanční subjekt součástí skupiny systémové povahy na úrovni Unie nebo na vnitrostátní úrovni ve finančním sektoru a sdílí systémy IKT;

b) faktorů souvisejících s riziky v oblasti IKT:

i) rizikového profilu finančního subjektu;

ii) prostředí hrozeb finančního subjektu;

iii) stupně závislosti zásadních nebo důležitých funkcí nebo jejich podpůrných funkcí finančního subjektu na systémech a procesech IKT;

iv) složitosti architektury IKT finančního subjektu;

v) služeb a funkcí IKT podporovaných poskytovateli služeb IKT z řad třetích stran a množství a druhu smluvních ujednání s poskytovateli služeb IKT z řad třetích stran nebo poskytovateli služeb IKT v rámci skupiny;

vi) výsledků všech přezkumů provedených orgány dohledu relevantních pro posouzení vyspělosti IKT finančního subjektu;

vii) vyspělosti plánů zachování provozu IKT a plánů reakce a obnovy v oblasti IKT;

viii) vyspělosti provozních opatření pro odhalování a zmírňování dopadů na bezpečnost IKT, včetně schopnosti:

1) trvale sledovat infrastrukturu IKT finančního subjektu;

2) zjišťovat události související s IKT v reálném čase;

3) analyzovat události uvedené v bodě 2;

4) včas a účinně reagovat na události uvedené v bodě 2;

ix) zda je finanční subjekt součástí skupiny působící ve finančním sektoru na úrovni Unie nebo na vnitrostátní úrovni, která sdílí systémy IKT.

Pro účely písmene a) bodu i) orgán pro penetrační testování na základě hrozeb pokud možno zohlední:

a) postavení finančního subjektu na trhu na úrovni Unie a na vnitrostátní úrovni;

b) rozsah činností, které finanční subjekt nabízí;

c) podíl služeb poskytovaných finančním subjektem nebo podíl činností prováděných na úrovni Unie a na vnitrostátní úrovni na trhu.

Pro účely písmene a) bodu v) orgán pro penetrační testování na základě hrozeb pokud možno zohlední:

a) zda finanční subjekt provozuje více než jeden obchodní model;

b) propojení různých obchodních procesů a souvisejících služeb.

2. Orgány pro penetrační testování na základě hrozeb vyžadují, aby všechny následující finanční subjekty provedly penetrační testování na základě hrozeb, pokud z posouzení uvedeného v odstavci 1 ve vztahu k finančnímu subjektu nevyplývá, že jeho dopad, hlediska finanční stability týkající se tohoto finančního subjektu nebo jeho rizikový profil v oblasti IKT provedení penetračního testování na základě hrozeb neodůvodňují:

a) úvěrové instituce splňující některou z těchto podmínek:

i) byly určeny jako globální systémově významné instituce (G-SVI) v souladu s článkem 131 směrnice Evropského parlamentu a Rady 2013/36/EU ([7]);

ii) byly určeny jako jiné systémově významné instituce (J-SVI) v souladu s článkem 131 směrnice 2013/36/EU;

iii) jsou součástí G-SVI nebo J-SVI;

([7]) Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) platební instituce, které v každém ze dvou kalendářních let předcházejících posouzení orgánem pro penetrační testování na základě hrozeb překročily celkovou hodnotu platebních transakcí ve výši 150 miliard EUR, jež jsou definovány v čl. 4 bodě 5 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ([8]);

c) instituce elektronických peněz, které v každém ze dvou kalendářních let předcházejících posouzení orgánem pro penetrační testování na základě hrozeb překročily buď 150 miliard EUR celkové hodnoty platebních transakcí ve smyslu čl. 4 bodu 5 směrnice (EU) 2015/2366, nebo 40 miliard EUR celkové hodnoty objemu elektronických peněz v oběhu;

d) centrální depozitáře cenných papírů;

e) ústřední protistrany;

f) obchodní systémy s elektronickým obchodním systémem, které splňují některé z následujících kritérií:

i) obchodní systém má nejvyšší podíl na trhu z hlediska obratu na vnitrostátní úrovni v každém ze dvou kalendářních let předcházejících posouzení orgánem pro penetrační testování na základě hrozeb, pokud jde o kterýkoli z následujících případů:

1) převoditelné cenné papíry ve smyslu čl. 4 odst. 1 bodu 44 písm. a) směrnice Evropského parlamentu a Rady 2014/65/EU ([9]);

2) převoditelné cenné papíry ve smyslu čl. 4 odst. 1 bodu 44 písm. b) směrnice 2014/65/EU;

3) deriváty ve smyslu čl. 2 odst. 1 bodu 29 nařízení Evropského parlamentu a Rady (EU) č. 600/2014 ([10]);

4) strukturované finanční produkty ve smyslu čl. 2 odst. 1 bodu 28 nařízení (EU) č. 600/2014;

5) povolenky na emise vymezené v příloze I oddíle C bodě 11 směrnice 2014/65/EU;

ii) obchodní systém má podíl na trhu z hlediska obratu na unijní úrovni, který v každém ze dvou kalendářních let předcházejících posouzení orgánem pro penetrační testování na základě hrozeb překračuje 5 %, pokud jde o kterýkoli z následujících případů:

1) akcie společností a další cenné papíry rovnocenné akciím společností, podílům v osobních společnostech či jiných subjektech, včetně cenných papírů nahrazujících akcie;

2) dluhopisy nebo jiné formy dluhových cenných papírů, včetně cenných papírů nahrazujících tyto cenné papíry;

3) deriváty ve smyslu čl. 2 odst. 1 bodu 29 nařízení (EU) č. 600/2014;

4) strukturované finanční produkty ve smyslu čl. 2 odst. 1 bodu 28 nařízení (EU) č. 600/2014;

5) povolenky na emise vymezené v příloze I oddíle C bodě 11 směrnice 2014/65/EU;

([8]) Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Nařízení Evropského parlamentu a Rady (EU) č. 600/2014 ze dne 15. května 2014 o trzích finančních nástrojů a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 173, 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) pojišťovny a zajišťovny, které splňují všechna následující kritéria:

i) mají předepsané hrubé pojistné vyšší než 1 500 000 000 EUR;

ii) mají technické rezervy vyšší než 10 000 000 000 EUR;

iii) pojišťovny vykonávající pouze činnosti životního pojištění nebo vykonávající činností životního i neživotního pojištění a jejichž celková aktiva přesahují 3,5 % součtu celkových aktiv oceněných v souladu s článkem 75 směrnice Evropského parlamentu a Rady 2009/138/ES ([11]) pojišťoven a zajišťoven usazených v členském státě.

Pro účely písmene f) bodu ii) se v případě, že je obchodní systém součástí skupiny sdílející systémy IKT nebo stejného poskytovatele služeb IKT v rámci skupiny, zohlední obrat smluv o cenných papírech a derivátech ve všech obchodních systémech patřících do stejné skupiny a usazených v Unii.

Pro účely písmene g) určí orgány pro penetrační testování na základě hrozeb podskupinu všech pojišťoven a zajišťoven podle kritérií stanovených v písmenu g) bodech i), ii) a iii). Pojišťovny a zajišťovny zahrnuté do této podskupiny jsou povinny provádět penetrační testování na základě hrozeb, pokud splňují také některé z následujících kritérií:

a) předepsané hrubé pojistné, které přesahuje 3 000 000 000 EUR;

b) technické rezervy, které přesahují 30 000 000 000 EUR;

c) celková aktiva, která přesahují 10 % součtu celkových aktiv oceněných v souladu s článkem 75 směrnice 2009/138/ES pojišťoven a zajišťoven usazených v členském státě.

3. Pokud kritéria stanovená v odstavci 2 splňuje více finančních subjektů patřících do stejné skupiny a sdílejících systémy IKT nebo pokud více finančních subjektů využívá stejného poskytovatele služeb IKT v rámci skupiny, orgány pro penetrační testování na základě hrozeb těchto finančních subjektů v souladu s čl. 16 odst. 2 rozhodnou, zda je pro tyto finanční subjekty relevantní požadavek na provádění penetračního testování na základě hrozeb na individuálním základě.

Pokud se orgán pro penetrační testování na základě hrozeb mateřského podniku skupiny finančních subjektů uvedených v prvním pododstavci liší od orgánů pro penetrační testování na základě hrozeb finančních subjektů skupiny, konzultují tento orgán orgány pro penetrační testování na základě hrozeb finančních subjektů patřících do této skupiny ohledně toho, zda je vhodné provádět penetrační testování na základě hrozeb na individuálním základě.

Článek 3

Vedoucí pracovníci pro testy, pokud jde o kybernetické týmy a penetrační testování na základě hrozeb

1. Orgán pro penetrační testování na základě hrozeb pověří kybernetický tým koordinací činností souvisejících s penetračním testováním na základě hrozeb. Kybernetický tým se skládá z vedoucích pracovníků pro testy, kteří jsou pověřeni dohledem nad jednotlivými testy v rámci penetračního testování na základě hrozeb.

2. Pro každý test určí orgán pro penetrační testování na základě hrozeb vedoucího pracovníka pro test a alespoň jednoho náhradníka.

3. Vedoucí pracovníci pro testy sledují, zda jsou dodržovány požadavky stanovené v tomto nařízení, a zajišťují jejich dodržování.

([11]) Směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. listopadu 2009 o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II) (Úř. věst. L 335, 17.12.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Vedoucí pracovníci pro testy sdělí kontaktní údaje kybernetického týmu finančnímu subjektu prostřednictvím oznámení uvedeného v čl. 9 odst. 1.

5. Orgán pro penetrační testování na základě hrozeb se účastní všech fází penetračního testování na základě hrozeb.

Článek 4

Organizační uspořádání finančních subjektů

1. Finanční subjekty jmenují vedoucího člena řídícího týmu, který odpovídá za každodenní řízení penetračního testování na základě hrozeb a za rozhodnutí a opatření řídícího týmu.

2. Finanční subjekty zavedou organizační a procesní opatření, která zajistí, aby:

a) přístup k informacím týkajícím se jakéhokoli plánovaného nebo probíhajícího penetračního testování na základě hrozeb byl omezen na základě potřeby „vědět jen to nejnutnější“ na řídící tým, vedoucí orgán, subjekty provádějící testování, poskytovatele operativních informací o hrozbách a orgán pro penetrační testování na základě hrozeb;

b) řídící tým konzultoval vedoucí pracovníky pro testy před zapojením kteréhokoli člena modrého týmu do penetračního testování na základě hrozeb;

c) řídící tým byl informován o každém zjištění v rámci penetračního testování na základě hrozeb zaměstnanci finančního subjektu nebo jeho poskytovatelů služeb z řad třetích stran; v případě potřeby eskalace reakce na vzniklý incident řídící tým tuto eskalaci omezil;

d) byla zavedena opatření týkající se zachování důvěrnosti penetračního testování na základě hrozeb, která se vztahují na zaměstnance finančního subjektu, zaměstnance dotčených poskytovatelů služeb IKT z řad třetích stran, subjekty provádějící testování a poskytovatele operativních informací o hrozbách;

e) řídící tým na požádání poskytl vedoucím pracovníkům pro testy veškeré informace týkající se penetračního testování na základě hrozeb;

f) zúčastněné strany zapojené do penetračního testování na základě hrozeb na toto testování odkazovaly pouze názvem kódu.

Článek 5

Řízení rizik pro penetrační testování na základě hrozeb

1. Během přípravné fáze uvedené v článku 9 řídící tým posoudí rizika spojená s testováním produkčních systémů zásadních nebo důležitých funkcí finančního subjektu za provozu, včetně možných dopadů na:

a) finanční sektor;

b) finanční stabilitu na úrovni Unie nebo na vnitrostátní úrovni.

Řídící tým tyto dopady v průběhu testování přezkoumá.

2. Pro účely posouzení a řízení rizik řídící tým zohlední přinejmenším následující typy rizik, které se týkají:

a) poskytnutí přístupu k citlivým informacím o finančním subjektu poskytovateli operativních informací o hrozbách a případně externím subjektům provádějícím testování;

b) nesouladu penetračního testování na základě hrozeb s nařízením (EU) 2022/2554 a s tímto nařízením, pokud tento nesoulad vede k chybějícímu osvědčení uvedenému v čl. 26 odst. 7 nařízení (EU) 2022/2554, včetně případů, kdy je tento nesoulad způsoben porušením důvěrnosti penetračního testování na základě hrozeb nebo neetickým chováním;

c) eskalace krizí a incidentů;

d) fáze aktivního testování metodou „červeného týmu“, včetně rizik spojených s přerušením kritických činností a poškozením dat v důsledku činnosti subjektů provádějících testování a jejich možných dopadů na třetí strany;

e) testování metodou „modrého týmu“, včetně rizik spojených s přerušením kritických činností a poškozením dat v důsledku činnosti modrého týmu a jejich možných dopadů na třetí strany;

f) neúplného obnovení systémů dotčených penetračním testováním na základě hrozeb.

Článek 6

Řízení rizik u společného nebo sdruženého penetračního testování na základě hrozeb

1. V případě sdruženého penetračního testování na základě hrozeb nebo společného penetračního testování na základě hrozeb provede řídící tým každého finančního subjektu vlastní posouzení rizik a stanoví vlastní opatření k řízení rizik.

2. Řídící tým určeného finančního subjektu uvedeného v čl. 16 odst. 3 písm. b) tohoto nařízení nebo finančního subjektu určeného v souladu s čl. 26 odst. 4 nařízení (EU) 2022/2554 posoudí rizika související se zapojením více finančních subjektů do penetračního testování na základě hrozeb. Řídící týmy zúčastněných finančních subjektů spolupracují s řídícím týmem určeného finančního subjektu na identifikaci potenciálních společných rizik.

Článek 7

Výběr poskytovatelů penetračního testování na základě hrozeb

1. Řídící tým přijme opatření k řízení rizik souvisejících s penetračním testováním na základě hrozeb a zejména zajistí, aby v případě každého penetračního testování na základě hrozeb:

a) poskytovatel operativních informací o hrozbách a externí subjekty provádějící testování poskytli řídícímu týmu podrobný životopis a kopie osvědčení, která jsou podle uznávaných tržních standardů vhodná pro výkon jejich činnosti;

b) poskytovatel operativních informací o hrozbách a externí subjekt provádějící testování byli řádně a plně kryti vhodným pojištěním odpovědnosti za škody při výkonu povolání, včetně rizik pochybení a nedbalosti;

c) poskytovatel operativních informací o hrozbách poskytl alespoň tři reference z předchozích úkolů v souvislosti s penetračním testováním a testováním metodou „červeného týmu“;

d) externí subjekty provádějící testování poskytly alespoň pět referencí z předchozích úkolů týkajících se penetračního testování a testování metodou „červeného týmu“;

e) zaměstnanci poskytovatele operativních informací o hrozbách přiděleného k penetračnímu testováním na základě hrozeb:

   i) zahrnovali alespoň vedoucího pracovníka s nejméně pětiletou praxí v oblasti operativních informací o hrozbách a alespoň jednoho dalšího člena s nejméně dvouletou praxí v oblasti operativních informací o hrozbách;

   ii) měli široký záběr a odpovídající úroveň odborných znalostí a dovedností, včetně:

      1) taktik, technik a postupů shromažďování operativních informací;

      2) geopolitických, technických a odvětvových znalostí;

      3) odpovídajících komunikačních dovedností, aby dokázali jasně informovat a podávat zprávy o výsledku svého zapojení;

   iii) byli kombinovaně zapojeni v nejméně třech předchozích úkolech v oblasti operativních informací o hrozbách v rámci penetračního testování a testování metodou „červeného týmu“;

   iv) současně nevykonávali žádné úkoly modrého týmu ani jiné služby, které by mohly představovat střet zájmů ve vztahu k finančnímu subjektu, poskytovateli služeb IKT z řad třetích stran nebo poskytovateli služeb IKT v rámci skupiny zapojenému do penetračního testováním na základě hrozeb, k němuž jsou přiděleni;

   v) byli odděleni od zaměstnanců téhož poskytovatele penetračního testování na základě hrozeb, který zajišťuje externí subjekty provádějící testování pro stejné penetrační testování na základě hrozeb, a nebyli těmto zaměstnancům podřízeni;

f) pokud jde o externí subjekty provádějící testování, červený tým přidělený k penetračnímu testování na základě hrozeb:

   i) se skládal minimálně z vedoucího pracovníka s nejméně pětiletou praxí v oblasti penetračního testování a testování metodou „červeného týmu“ a z nejméně dvou dalších subjektů provádějících testování, z nichž každý má nejméně dvouletou praxi v oblasti penetračního testování a testování metodou „červeného týmu“;

   ii) měl široký záběr a odpovídající úroveň odborných znalostí a dovedností, včetně znalostí o podnikání finančního subjektu, průzkumu, řízení rizik, vývoji využití, fyzickém průniku, sociálním inženýrství, analýze zranitelností, jakož i odpovídající komunikační dovednosti, aby dokázal jasně informovat a podávat zprávy o výsledku svého zapojení;

   iii) byl kombinovaně zapojen v nejméně pěti předchozích úkolech týkajících se penetračního testování a testování metodou „červeného týmu“;

   iv) nebyl zaměstnán poskytovatelem operativních informací o hrozbách ani neposkytoval služby poskytovateli operativních informací o hrozbách, který současně plní úkoly modrého týmu buď pro finanční subjekt, nebo pro poskytovatele služeb IKT z řad třetích stran, nebo pro poskytovatele služeb IKT v rámci skupiny, který je zapojen do penetračního testování na základě hrozeb;

   v) byl oddělen od všech zaměstnanců téhož poskytovatele penetračního testování na základě hrozeb, který současně poskytuje služby týkající se operativních informací o hrozbách pro stejné penetrační testování na základě hrozeb;

g) subjekty provádějící testování a poskytovatel operativních informací o hrozbách provedli na konci testování postupy obnovy, včetně bezpečného vymazání informací týkajících se hesel, přihlašovacích údajů a dalších tajných klíčů, které byly během penetračního testování na základě hrozeb ohroženy, informování finančního subjektu o ohrožených účtech bezpečnou cestou a bezpečného shromažďování, ukládání, správy a likvidace dalších údajů shromážděných během testování;

h) kromě postupů obnovy na konci testování uvedených v písmenu g) provedly subjekty provádějící testování následující postupy obnovy:

   i) deaktivaci ovládání a řízení;

   ii) nouzové vypínače („kill switches“) pro rozsah a datum;

   iii) odstranění zadních vrátek a dalšího škodlivého softwaru;

   iv) oznámení o možném narušení;

   v) postupy pro budoucí obnovu záloh, které se mohou týkat škodlivého softwaru nebo nástrojů nainstalovaných během testu;

   vi) sledování činnosti modrého týmu a informování řídícího týmu o případných zjištěních;

i) subjekty provádějící testování a poskytovatel operativních informací o hrozbách neprováděli žádnou z následujících činností a ani se na nich nepodíleli:

   i) neoprávněné zničení zařízení finančního subjektu a jeho případných poskytovatelů služeb IKT z řad třetích stran;

   ii) neřízené úpravy informací a aktiv IKT finančního subjektu a jeho případných poskytovatelů služeb IKT z řad třetích stran;

   iii) záměrné narušení kontinuity zásadních nebo důležitých funkcí finančního subjektu;

   iv) neoprávněné zahrnutí systémů mimo stanovený rozsah;

   v) neoprávněné zveřejnění výsledků testů.

2. Řídící tým vede záznamy o dokumentaci poskytnuté subjekty provádějícími testování a poskytovateli operativních informací o hrozbách, aby prokázal soulad s odst. 1 písm. a) až f).

Finanční subjekty mohou ve výjimečných případech uzavřít smlouvu s externími subjekty provádějícími testování a poskytovateli operativních informací o hrozbách, kteří nesplňují jeden nebo více požadavků uvedených v odst. 1 písm. a) až f), za předpokladu, že tyto finanční subjekty přijmou opatření, která jsou vhodná ke zmírnění rizik souvisejících s nesplněním těchto požadavků, a o těchto opatřeních pořídí záznamy.

Článek 8

Specifické vlastnosti společného nebo sdruženého penetračního testování na základě hrozeb

1. Pokud vedoucí orgán pro penetrační testování na základě hrozeb nerozhodne jinak, v případě, že se na společném nebo sdruženém penetračním testování na základě hrozeb podílí několik finančních subjektů určených v souladu s čl. 16 odst. 2 nebo 4, postupuje každý finanční subjekt podle všech kroků uvedených v článcích 9 až 15.

2. Není-li v tomto nařízení stanoveno jinak, v případě, že se na společném nebo sdruženém penetračním testování na základě hrozeb podle čl. 16 odst. 3 nebo 5 podílí více orgánů pro penetrační testování na základě hrozeb, se odkazy na „orgán pro penetrační testování na základě hrozeb“ uvedené v článcích 9 až 15 považují za odkazy na vedoucí orgán pro penetrační testování na základě hrozeb pro toto společné nebo sdružené penetrační testování na základě hrozeb.

Článek 9

Přípravná fáze

1. Finanční subjekt určený podle čl. 26 odst. 8 třetího pododstavce nařízení (EU) 2022/2554 zahájí penetrační testování na základě hrozeb po oznámení orgánu pro penetrační testování na základě hrozeb, že má být penetrační testování na základě hrozeb provedeno.

2. Finanční subjekt do tří měsíců od obdržení oznámení uvedeného v odstavci 1 předloží vedoucím pracovníkům pro testy všechny následující informace k zahájení penetračního testování na základě hrozeb:

a) zásady projektu zahrnující plán projektu na vysoké úrovni, které obsahují informace uvedené v příloze I;

b) kontaktní údaje vedoucího člena řídícího týmu;

c) informace o zamýšleném použití interních nebo externích subjektů provádějících testování, případně obou, jak je uvedeno v článku 15;

d) informace o komunikačních kanálech, které se mají používat během penetračního testování na základě hrozeb;

e) název kódu penetračního testování na základě hrozeb.

3. Pokud jsou informace uvedené v odst. 2 písm. a) až e) úplné a zajišťují vhodné a efektivní provádění penetračního testování na základě hrozeb, orgán pro penetrační testování na základě hrozeb potvrdí informace finančního subjektu k zahájení penetračního testování na základě hrozeb a oznámí to finančnímu subjektu.

4. Po potvrzení informací k zahájení penetračního testování na základě hrozeb orgánem pro penetrační testování na základě hrozeb finanční subjekt zřídí řídící tým, který bude vedoucímu členovi řídícího týmu pomáhat při plnění jeho následujících úkolů:

a) stanovení komunikačních kanálů a postupů v rámci řídícího týmu pro komunikaci se subjekty provádějícími testování a poskytovateli operativních informací o hrozbách ve všech záležitostech souvisejících s penetračním testováním na základě hrozeb;

b) informování vedoucího orgánu finančního subjektu o průběhu penetračního testování na základě hrozeb a souvisejících rizicích;

c) přijímání rozhodnutí na základě odborných znalostí v rámci penetračního testování na základě hrozeb;

d) provádění penetračního testování na základě hrozeb v souladu s tímto nařízením;

e) výběr poskytovatele operativních informací o hrozbách pro penetrační testování na základě hrozeb;

f) výběr externích subjektů provádějících testování, interních subjektů provádějících testování nebo obou;

g) vypracování dokumentu, který vymezuje rozsah.

5. Pokud se orgán pro penetrační testování na základě hrozeb domnívá, že původní složení řídícího týmu a jeho případné následné změny jsou vhodné pro plnění úkolů uvedených v odstavci 4, orgán pro penetrační testování na základě hrozeb potvrdí platnost řídícího týmu a oznámí to vedoucímu členovi řídícího týmu.

6. Finanční subjekt předloží dokument, který vymezuje rozsah a který obsahuje všechny informace uvedené v příloze II, vedoucím pracovníkům pro testy do šesti měsíců od obdržení oznámení od orgánu pro penetrační testování na základě hrozeb uvedeného v odstavci 1. Vedoucí orgán finančního subjektu schvaluje dokument, který vymezuje rozsah.

7. Finanční subjekty zváží následující kritéria pro zahrnutí zásadních nebo důležitých funkcí do rozsahu penetračního testování na základě hrozeb:

a) význam nebo důležitost funkce a její možný dopad na finanční sektor a finanční stabilitu na úrovni Unie a na vnitrostátní úrovni;

b) význam funkce pro každodenní obchodní operace finančního subjektu;

c) nahraditelnost funkce;

d) propojenost s ostatními funkcemi;

e) zeměpisná poloha funkce;

f) odvětvová závislost ostatních subjektů na funkci;

g) operativní informace o hrozbách týkající se funkce, pokud jsou k dispozici.

8. Řídící tým poskytuje informace k zahájení penetračního testování na základě hrozeb a dokument, který vymezuje rozsah, subjektům provádějícím testování a poskytovatelům operativních informací o hrozbách, jakmile jsou s nimi uzavřeny smlouvy. Řídící tým informuje subjekty provádějící testování a poskytovatele operativních informací o hrozbách o postupu testování, který je třeba dodržet.

9. Finanční subjekt zajistí, aby před zahájením fáze testování bylo dokončeno uzavření smlouvy se subjekty provádějícími testování a poskytovateli operativních informací o hrozbách nebo jejich přidělení.

10. Před zahájením fáze testování konzultuje řídící tým s vedoucími pracovníky pro testy posouzení rizik penetračního testování na základě hrozeb a opatření k řízení rizik. Řídící tým přezkoumá posouzení rizik nebo opatření k řízení rizik, pokud se orgán pro penetrační testování na základě hrozeb domnívá, že dostatečně neřeší rizika penetračního testování na základě hrozeb.

11. Řídící tým posoudí, zda poskytovatelé operativních informací o hrozbách a subjekty provádějící testování, o jejichž zapojení do penetračního testování na základě hrozeb uvažuje, splňují požadavky stanovené v článku 27 nařízení (EU) 2022/2554 a v čl. 7 odst. 1 tohoto nařízení, a výsledek tohoto posouzení zdokumentuje. Řídící tým vybere poskytovatele operativních informací o hrozbách v souladu s tímto posouzením a se svými postupy řízení rizik. Před uzavřením smlouvy s vybranými poskytovateli operativních informací o hrozbách a externími subjekty provádějícími testování předloží řídící tým vedoucím pracovníkům pro testy důkazy o tom, že tito poskytovatelé operativních informací o hrozbách a subjekty provádějící testování splňují požadavky stanovené v článku 27 nařízení (EU) 2022/2554 a v čl. 7 odst. 1 tohoto nařízení. Řídící tým nepokračuje v uzavírání smluv s vybranými poskytovateli operativních informací o hrozbách a externími subjekty provádějícími testování, pokud se orgán pro penetrační testování na základě hrozeb domnívá, že vybraní poskytovatelé operativních informací o hrozbách a externí subjekty provádějící testování nesplňují požadavky stanovené v článku 27 nařízení (EU) 2022/2554, požadavky stanovené v čl. 7 odst. 1 tohoto nařízení nebo další požadavky vyplývající z vnitrostátních bezpečnostních právních předpisů v souladu s právem Unie, nebo pokud finanční subjekt nesplňuje požadavky uvedené v čl. 7 odst. 2 prvním pododstavci tohoto nařízení nebo pokud nejsou splněny okolnosti uvedené v čl. 7 odst. 2 druhém pododstavci tohoto nařízení.

12. Pokud je dokument, který vymezuje rozsah, úplný a zajišťuje provedení vhodného a účinného penetračního testování na základě hrozeb, orgán pro penetrační testování na základě hrozeb tento dokument schválí a informuje o tom vedoucího člena řídícího týmu.

Článek 10

Fáze testování: operativní informace o hrozbách

1. Po schválení dokumentu, který vymezuje rozsah, orgánem pro penetrační testování na základě hrozeb poskytovatel operativních informací o hrozbách analyzuje obecné a odvětvové operativní informace o hrozbách relevantní pro finanční subjekt. Pokud orgán pro penetrační testování na základě hrozeb poskytl generické prostředí hrozeb pro finanční sektor členského státu, může poskytovatel operativních informací o hrozbách toto prostředí použít jako výchozí bod pro vnitrostátní prostředí hrozeb. Poskytovatel operativních informací o hrozbách identifikuje kybernetické hrozby a stávající nebo potenciální zranitelnosti týkající se finančního subjektu. Poskytovatel operativních informací o hrozbách dále shromažďuje informace o konkrétních, využitelných a do kontextu zasazených operativních informacích o cílech a hrozbách, které se týkají finančního subjektu, a analyzuje je, a to i prostřednictvím konzultací s řídícím týmem a vedoucími pracovníky pro testy.

2. Poskytovatel operativních informací o hrozbách předloží příslušné hrozby a cílené operativní informace o hrozbách a navrhne požadované scénáře řídícímu týmu, subjektům provádějícím testy a vedoucím pracovníkům pro testy. Navrhované scénáře se liší s ohledem na identifikované aktéry hrozeb a související taktiky, techniky a postupy a zaměřují se na každou zásadní nebo důležitou funkci v rámci penetračního testování na základě hrozeb.

3. Vedoucí člen řídícího týmu vybere nejméně tři scénáře pro provedení penetračního testování na základě hrozeb na základě všech následujících prvků:

a) doporučení poskytovatele operativních informací o hrozbách a povahy jednotlivých scénářů na základě hrozeb;

b) vstupů poskytnutých vedoucími pracovníky pro testy;

c) proveditelnosti navržených scénářů na základě odborného úsudku subjektů provádějících testování;

d) velikosti, složitosti a celkového rizikového profilu finančního subjektu a povahy, rozsahu a složitosti jeho služeb, činností a operací.

4. Maximálně jeden z vybraných scénářů nemusí být založen na hrozbách a může být založen na výhledové a potenciálně fiktivní hrozbě s vysokou prediktivní, anticipační, oportunistickou nebo prospektivní hodnotou vzhledem k předpokládanému vývoji prostředí hrozeb, které se týkají finančního subjektu.

Aniž jsou u společného penetračního testování na základě hrozeb dotčeny scénáře zaměřené přímo na zásadní nebo důležité funkce finančních subjektů zapojených do testování, musí alespoň jeden scénář zahrnovat příslušné základní systémy, procesy a technologie IKT poskytovatele služeb IKT z řad třetích stran, které podporují zásadní nebo důležité funkce finančních subjektů v rozsahu testování.

Pokud se jedná o sdružené penetrační testování na základě hrozeb zahrnující poskytovatele služeb IKT v rámci skupiny, aniž jsou dotčeny scénáře zaměřené přímo na zásadní nebo důležité funkce finančních subjektů zapojených do testu, musí alespoň jeden scénář zahrnovat příslušné základní systémy, procesy a technologie IKT poskytovatele služeb IKT v rámci skupiny, které podporují zásadní nebo důležité funkce finančních subjektů v rozsahu testování.

5. Poskytovatel operativních informací o hrozbách poskytne řídícímu týmu zprávu o cílených operativních informacích o hrozbách, včetně scénářů vybraných podle odstavců 3 a 4. Zpráva o operativních informacích o hrozbách obsahuje informace uvedené v příloze III.

6. Řídící tým předloží zprávu o cílených operativních informacích o hrozbách vedoucímu pracovníkovi pro testy ke schválení. Pokud je zpráva o cílených operativních informacích o hrozbách úplná a zajišťuje provedení účinného penetračního testování na základě hrozeb, orgán pro penetrační testování na základě hrozeb zprávu o cílených operativních informacích o hrozbách schválí a informuje o tom vedoucího člena řídícího týmu.

Článek 11

Fáze testování: testování metodou „červeného týmu“

1. Po schválení zprávy o cílených operativních informacích o hrozbách orgánem pro penetrační testování na základě hrozeb připraví subjekty provádějící testování plán testování metodou „červeného týmu“, který obsahuje informace uvedené v příloze IV. Jako základ pro tvorbu scénářů útoku použijí subjekty provádějící testování dokument, který vymezuje rozsah, a zprávu o cílených operativních informacích o hrozbách.

2. Subjekty provádějící testování konzultují s řídícím týmem, poskytovatelem operativních informací o hrozbách a vedoucími pracovníky pro testy plán testování metodou „červeného týmu“, včetně komunikace, procesního a projektového řízení, přípravy a případů použití pro aktivaci podpory a dohod o podávání zpráv řídícímu týmu a vedoucím pracovníkům pro testy.

3. Pokud je plán testování metodou „červeného týmu“ úplný a zajišťuje provedení účinného penetračního testování na základě hrozeb, řídící tým a orgán pro penetrační testování na základě hrozeb schválí plán testování metodou „červeného týmu“ a informuje o tom vedoucího člena řídícího týmu.

4. Po schválení plánu testování metodou „červeného týmu“ podle odstavce 3 provedou subjekty provádějící testování penetrační testování na základě hrozeb během fáze aktivního testování metodou „červeného týmu“.

5. Doba trvání fáze aktivního testování metodou „červeného týmu“ je úměrná rozsahu penetračního testování na základě hrozeb, rozsahu, činnosti, složitosti a počtu finančních subjektů a poskytovatelů služeb IKT z řad třetích stran nebo poskytovatelů služeb IKT v rámci skupiny zapojených do penetračního testování na základě hrozeb a v každém případě trvá nejméně dvanáct týdnů. Scénáře útoku lze provádět postupně nebo současně. Řídící tým, poskytovatel operativních informací o hrozbách, subjekty provádějící testování a vedoucí pracovníci pro testy se dohodnou na ukončení fáze aktivního testování metodou „červeného týmu“.

6. Vedoucí člen řídícího týmu a vedoucí pracovníci pro testy schvalují veškeré změny plánu testování metodou „červeného týmu“ po jeho schválení, včetně časového plánu, rozsahu, cílových systémů nebo příznaků pod podmínkou, že plán testování metodou „červeného týmu“ zůstane úplný a umožní provedení účinného penetračního testování na základě hrozeb.

7. Během celé fáze aktivního testování metodou „červeného týmu“ podávají subjekty provádějící testování nejméně jednou týdně řídícímu týmu a vedoucím pracovníkům pro testy zprávy o pokroku dosaženém při penetračním testování na základě hrozeb a poskytovatel operativních informací o hrozbách musí být na žádost řídícího týmu k dispozici pro konzultace a za účelem poskytnutí dalších operativních informací o hrozbách.

8. Řídící tým včas zajistí podporu navrženou na základě plánu testování metodou „červeného týmu“. Po schválení řídícím týmem a vedoucími pracovníky pro testy může být podpora přidána nebo upravena.

9. V případě, že dojde k odhalení testovacích činností kterýmkoli zaměstnancem finančního subjektu nebo jeho poskytovatelů služeb IKT z řad třetích stran nebo případně poskytovatelů služeb IKT v rámci skupiny, řídící tým po konzultaci se subjekty provádějícími testování, aniž je dotčen odstavec 10, navrhne a předloží vedoucím pracovníkům pro testy k potvrzení opatření umožňující pokračování penetračního testování na základě hrozeb, která zajišťují jeho důvěrnost.

10. Za výjimečných okolností, které zvyšují rizika dopadu na data, poškození aktiv a narušení zásadních nebo důležitých funkcí, služeb nebo operací samotného finančního subjektu, jeho poskytovatelů služeb IKT z řad třetích stran nebo poskytovatelů služeb IKT v rámci skupiny, nebo narušení jeho protistran nebo finančního sektoru, může vedoucí člen řídícího týmu pozastavit penetrační testování na základě hrozeb nebo v krajním případě, kdy pokračování penetračního testování na základě hrozeb není jinak možné, a po předchozím schválení orgánem pro penetrační testování na základě hrozeb, pokračovat v penetračním testování na základě hrozeb s využitím omezeného testování metodou „fialového týmu“. Doba trvání omezeného testování metodou „fialového týmu“ se započítává do minimální dvanáctitýdenní doby trvání fáze aktivního testování metodou „červeného týmu“ uvedené v odstavci 5.

Článek 12

Fáze ukončení

1. Po skončení fáze aktivního testování metodou „červeného týmu“ informuje vedoucí člen řídícího týmu modrý tým, že proběhlo penetrační testování na základě hrozeb.

2. Do čtyř týdnů od ukončení fáze aktivního testování metodou „červeného týmu“ předloží subjekty provádějící testování řídícímu týmu zprávu o testování metodou „červeného týmu“, která obsahuje informace uvedené v příloze V.

3. Řídící tým bez zbytečného odkladu poskytne zprávu o testování metodou „červeného týmu“ modrému týmu a vedoucím pracovníkům pro testy.

Na žádost vedoucích pracovníků pro testy neobsahuje zpráva uvedená v prvním pododstavci citlivé informace.

4. Po obdržení zprávy o testování metodou „červeného týmu“, nejpozději však deset týdnů po ukončení fáze aktivního testování metodou „červeného týmu“, předloží modrý tým řídícímu týmu zprávu o testování metodou „modrého týmu“ obsahující informace uvedené v příloze VI. Řídící tým bez zbytečného odkladu poskytne zprávu o testování metodou „modrého týmu“ subjektům provádějícím testování a vedoucím pracovníkům pro testy.

Na žádost vedoucích pracovníků pro testy neobsahuje zpráva uvedená v prvním pododstavci citlivé informace.

5. Nejpozději deset týdnů po skončení fáze aktivního testování metodou „červeného týmu“ modrý tým a subjekty provádějící testování zopakují útočné a obranné akce provedené během penetrační testování na základě hrozeb. Řídící tým rovněž provede testování metodou „fialového týmu“ v oblasti témat společně určených modrým týmem a subjekty provádějícími testování, a to na základě zranitelností zjištěných během testu, a případně v záležitostech, které nebylo možné otestovat během fáze aktivního testování metodou „červeného týmu“.

6. Po dokončení zopakování a testování metodou „fialového týmu“ si řídící tým, modrý tým, subjekty provádějící testování a poskytovatelé operativních informací o hrozbách vzájemně poskytnou zpětnou vazbu k procesu penetračního testování na základě hrozeb. Vedoucí pracovníci pro testy mohou poskytnout zpětnou vazbu.

7. Jakmile orgán pro penetrační testování na základě hrozeb oznámí vedoucímu členovi řídícího týmu, že vyhodnotil, že zpráva o testování metodou „modrého týmu“ a zpráva o testování metodou „červeného týmu“ obsahují informace stanovené v přílohách V a VI, předloží finanční subjekt do osmi týdnů orgánu pro penetrační testování na základě hrozeb podle čl. 26 odst. 6 nařízení (EU) 2022/2554 ke schválení zprávu shrnující příslušná zjištění penetračního testování na základě hrozeb, která obsahuje prvky stanovené v příloze VII.

Na žádost orgánu pro penetrační testování na základě hrozeb neobsahuje zpráva uvedená v prvním pododstavci citlivé informace.

Článek 13

Plán nápravných opatření

1. Do osmi týdnů od oznámení uvedeného v čl. 12 odst. 7 tohoto nařízení poskytne finanční subjekt plány nápravných opatření a dokumentaci uvedenou v čl. 26 odst. 6 nařízení (EU) 2022/2554 orgánu pro penetrační testování na základě hrozeb a příslušnému orgánu finančního subjektu, pokud se tyto orgány liší.

2. Plán nápravných opatření uvedený v odstavci 1 obsahuje pro každé zjištění, které bylo učiněno v rámci penetračního testování na základě hrozeb:

a) popis zjištěných nedostatků;

b) popis navrhovaných nápravných opatření, jejich seřazení podle priorit a předpokládaného dokončení, včetně případných opatření ke zlepšení identifikace, ochrany, detekce a schopnosti reakce;

c) analýzu kořenových příčin;

d) zaměstnance nebo funkce finančního subjektu odpovědné za provedení navrhovaných nápravných opatření nebo zlepšení;

e) rizika spojená s neprovedením opatření uvedených v písmenu b) a případně rizika spojená s provedením těchto opatření.

Článek 14

Osvědčení

1. Osvědčení uvedené v čl. 26 odst. 7 nařízení (EU) 2022/2554 obsahuje informace uvedené v příloze VIII.

2. Pokud se na penetračním testování na základě hrozeb podílí více orgánů pro penetrační testování na základě hrozeb, poskytne vedoucí orgán pro penetrační testování na základě hrozeb testovaným finančním subjektům osvědčení podle čl. 26 odst. 7 nařízení (EU) 2022/2554.

Článek 15

Využití interních subjektů provádějících testování

1. Finanční subjekty zavedou pro využití interních subjektů provádějících testování všechna následující opatření:

a) vypracování a zavedení politiky řízení interních subjektů provádějících testování v rámci penetračního testování na základě hrozeb;

b) opatření, která zajistí, že využití interních subjektů provádějících testování k provedení penetračního testování na základě hrozeb nebude mít negativní dopad na obecnou obranyschopnost nebo odolnost finančního subjektu vůči incidentům souvisejícím s IKT nebo významně neovlivní dostupnost zdrojů přidělených na úkoly související s IKT během penetračního testování na základě hrozeb;

c) opatření k zajištění toho, aby interní subjekty provádějící testování měly dostatečné zdroje a schopnosti k provedení penetračního testování na základě hrozeb;

politika uvedená v písmeni a):

a) zahrnuje kritéria pro posouzení vhodnosti, způsobilosti a potenciálního střetu zájmů interních subjektů provádějících testování a specifikuje povinnosti vedení v procesu testování;

b) je zdokumentována a pravidelně přezkoumávána;

c) zajišťuje, aby interní tým pro testování zahrnoval vedoucího člena pro testování a nejméně dva další členy;

d) vyžaduje, aby všichni členové týmu pro testování byli po dobu předchozích dvanácti měsíců zaměstnáni u finančního subjektu nebo u poskytovatele služeb IKT v rámci skupiny;

e) zahrnuje ustanovení o školení, jak provádět penetrační testování a testování metodou „červeného týmu“ za použití interních subjektů provádějících testování.

2. Pokud orgán pro penetrační testování na základě hrozeb schvaluje využití interních subjektů provádějících testování v souladu s čl. 27 odst. 2 písm. a) nařízení (EU) 2022/2554, musí orgán pro penetrační testování na základě hrozeb zohlednit požadavky stanovené v čl. 7 odst. 1 tohoto nařízení.

3. Při využití interních subjektů provádějících testování finanční subjekt zajistí, aby jejich využití bylo uvedeno v následujících dokumentech:

a) informacích k zahájení testu uvedených v článku 9;

b) zprávě o testování metodou „červeného týmu“ uvedené v čl. 12 odst. 2;

c) zprávě shrnující příslušná zjištění penetračního testování na základě hrozeb uvedené v čl. 26 odst. 6 nařízení (EU) 2022/2554.

4. Subjekty provádějící testování zaměstnané poskytovatelem služeb IKT v rámci skupiny se považují za interní subjekty provádějící testování finančního subjektu.

Článek 16

Spolupráce a vzájemné uznávání

1. Pro účely provádění penetračního testování na základě hrozeb ve vztahu k finančnímu subjektu, který poskytuje služby ve více než jednom členském státě, a to i prostřednictvím pobočky, jeho orgán pro penetrační testování na základě hrozeb:

a) určí, které orgány pro penetrační testování na základě hrozeb v hostitelských členských státech budou zapojeny, přičemž zohlední, zda je v hostitelských členských státech vykonávána jedna nebo více zásadních nebo důležitých funkcí nebo zda jsou tyto funkce sdíleny napříč hostitelskými členskými státy;

b) informuje orgány pro penetrační testování na základě hrozeb určené v souladu s písmenem a) o rozhodnutí provést penetrační testování na základě hrozeb u finančního subjektu;

c) pokud se orgány pro penetrační testování na základě hrozeb nedohodnou jinak, vede penetrační testování na základě hrozeb orgán finančního subjektu.

Orgány pro penetrační testování na základě hrozeb hostitelských členských států mohou do dvaceti pracovních dnů od obdržení informace o budoucím konání penetračního testování na základě hrozeb buď vyjádřit svůj zájem sledovat penetrační testování na základě hrozeb jako pozorovatelé, nebo určit vedoucího pracovníka pro testy k účasti na penetračním testování na základě hrozeb. Vedoucí orgán pro penetrační testování na základě hrozeb poskytne všem orgánům pro penetrační testování na základě hrozeb, které v penetračním testování na základě hrozeb působí jako pozorovatelé, dokument, který vymezuje rozsah, souhrnnou zprávu o testu, plán nápravných opatření a osvědčení.

Vedoucí orgán pro penetrační testování na základě hrozeb koordinuje všechny zúčastněné orgány pro penetrační testování na základě hrozeb v průběhu celého testu a přijímá veškerá rozhodnutí nezbytná k řádnému a účinnému provedení penetračního testování na základě hrozeb. Vedoucí orgán pro penetrační testování na základě hrozeb může stanovit maximální počet zúčastněných orgánů pro penetrační testování na základě hrozeb, pokud by jinak mohlo být ohroženo účinné provádění penetračního testování na základě hrozeb.

2. Pokud finanční subjekt využívá stejného poskytovatele služeb IKT v rámci skupiny jako finanční subjekty usazené v jiných členských státech nebo patří do skupiny a sdílí systémy IKT s finančními subjekty téže skupiny usazenými v jiných členských státech, orgán pro penetrační testování na základě hrozeb finančního subjektu kontaktuje orgány pro penetrační testování na základě hrozeb ostatních finančních subjektů, které využívají stejného poskytovatele služeb IKT v rámci skupiny nebo sdílejí systémy IKT jako součást skupiny, a posoudí s nimi proveditelnost a vhodnost provedení sdruženého penetračního testování na základě hrozeb u těchto finančních subjektů. Sdružené penetrační testování na základě hrozeb se upřednostní před individuálním penetračním testováním na základě hrozeb, pokud to může vést ke snížení nákladů a zdrojů finančních subjektů a orgánů pro penetrační testování na základě hrozeb za předpokladu, že tím není dotčena spolehlivost a účinnost testování.

3. Pro účely provedení sdruženého penetračního testování na základě hrozeb:

a) orgány pro penetrační testování na základě hrozeb finančních subjektů se dohodnou, který finanční subjekt bude určen k provedení penetračního testování na základě hrozeb, a to s ohledem na strukturu skupiny a účinnost testu;

b) orgán pro penetrační testování na základě hrozeb finančního subjektu určeného podle písmene a) vede penetrační testování na základě hrozeb, pokud se orgány pro penetrační testování na základě hrozeb finančních subjektů účastnících se sdruženého penetračního testování na základě hrozeb nedohodnou jinak;

c) orgány pro penetrační testování na základě hrozeb finančních subjektů jiných než určený finanční subjekt, které vedou sdružené penetrační testování na základě hrozeb, mohou buď vyjádřit svůj zájem sledovat penetrační testování na základě hrozeb jako pozorovatelé, nebo přidělit vedoucího pracovníka pro testy pro toto penetrační testování na základě hrozeb.

Vedoucí orgán pro penetrační testování na základě hrozeb koordinuje všechny orgány pro penetrační testování na základě hrozeb zapojené do sdruženého penetračního testování na základě hrozeb a přijímá veškerá rozhodnutí nezbytná k řádnému a účinnému provádění sdruženého penetračního testování na základě hrozeb.

4. Pokud finanční subjekt zamýšlí provést společné penetrační testování na základě hrozeb podle čl. 26 odst. 4 nařízení (EU) 2022/2554, do něhož se případně zapojí finanční subjekty usazené v jiných členských státech, kontaktuje jeho orgán pro penetrační testování na základě hrozeb orgány pro penetrační testování na základě hrozeb ostatních finančních subjektů a společně s nimi posoudí proveditelnost a vhodnost provedení společného penetračního testování na základě hrozeb u těchto finančních subjektů v souladu s čl. 26 odst. 4 nařízení (EU) 2022/2554.

5. Pro účely provedení společného penetračního testování na základě hrozeb podle čl. 26 odst. 4 nařízení (EU) 2022/2554:

a) orgány pro penetrační testování na základě hrozeb finančních subjektů se dohodnou na tom, který finanční subjekt bude určen k vedení společného penetračního testování na základě hrozeb, s ohledem na služby IKT poskytované poskytovatelem služeb IKT z řad třetích stran finančním subjektům a na účinnost testu;

b) orgán pro penetrační testování na základě hrozeb finančního subjektu určeného podle písmene a) vede penetrační testování na základě hrozeb, pokud se orgány pro penetrační testování na základě hrozeb finančních subjektů účastnících se společného penetračního testování na základě hrozeb nedohodnou jinak;

c) orgány pro penetrační testování na základě hrozeb finančních subjektů jiných než určený finanční subjekt, který vede společné penetrační testování na základě hrozeb, mohou buď vyjádřit svůj zájem sledovat penetrační testování na základě hrozeb jako pozorovatelé, nebo přidělit vedoucího pracovníka pro testy pro toto penetrační testování na základě hrozeb.

Vedoucí orgán pro penetrační testování na základě hrozeb koordinuje všechny orgány pro penetrační testování na základě hrozeb zapojené do společného penetračního testování na základě hrozeb a přijímá veškerá rozhodnutí nezbytná k řádnému a účinnému provádění společného penetračního testování na základě hrozeb.

6. Pokud se ve vztahu k finančnímu subjektu, který má provést penetrační testování na základě hrozeb, jeho orgán pro penetrační testování na základě hrozeb liší od jeho příslušného orgánu uvedeného v článku 46 nařízení (EU) 2022/2554, poskytují si tyto orgány veškeré relevantní informace týkající se všech záležitostí souvisejících s penetračním testováním na základě hrozeb pro účely provedení penetračního testování na základě hrozeb nebo pro plnění svých povinností v souladu s uvedeným nařízením.

Článek 17

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 13. února 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

Obsah zásad projektu (čl. 9 odst. 2 písm. a))

Údaj	Požadované informace
Osoba odpovědná za plán projektu, tj. vedoucí člen řídícího týmu	Jméno Kontaktní údaje
Subjekty provádějící testování	☐ interní ☐ externí ☐ interní i externí
Komunikační kanály vybrané v souladu s čl. 9 odst. 2 písm. d) a čl. 9 odst. 4 písm. a), včetně: a) šifrování e-mailu, které se použije b) online datové místnosti, které se použijí c) výměna rychlých zpráv, která se použije	
Název kódu penetračního testování na základě hrozeb	
Případné zásadní nebo důležité funkce, které finanční subjekt vykonává v jiných členských státech	1. seznam zásadních nebo důležitých funkcí vykonávaných v jiném členském státě 2. u každé zásadní nebo důležité funkce uvedení členského státu nebo států, ve kterých jsou vykonávány
Případné zásadní nebo důležité funkce podporované poskytovateli služeb IKT z řad třetích stran	3. seznam zásadních nebo důležitých funkcí podporovaných poskytovateli služeb IKT z řad třetích stran 4. u každé funkce identifikace poskytovatele služeb IKT z řad třetích stran
Očekávaná lhůta pro dokončení:	
1) přípravné fáze v souladu s článkem 9	rrrr-mm-dd
2) fáze testování v souladu s články 10 a 11	rrrr-mm-dd
3) fáze ukončení v souladu s článkem 12	rrrr-mm-dd
4) plánu nápravných opatření v souladu s článkem 13	rrrr-mm-dd

PŘÍLOHA II

Obsah dokumentu, který vymezuje rozsah (čl. 9 odst. 6)

1. Dokument, který vymezuje rozsah, musí obsahovat seznam všech zásadních nebo důležitých funkcí, které finanční subjekt určil.

2. Pro každou určenou zásadní nebo důležitou funkci se uvedou následující informace:
   a) pokud zásadní nebo důležitá funkce není zahrnuta do rozsahu penetračního testování na základě hrozeb, uvedení důvodů, proč není zahrnuta;
   b) pokud je zásadní nebo důležitá funkce do rozsahu penetračního testování na základě hrozeb zahrnuta:
      i) vysvětlení důvodů jejího zahrnutí;
      ii) určený(é) systém(y) IKT, který(é) podporuje(í) tuto zásadní nebo důležitou funkci;
      iii) pro každý určený systém IKT:
         1. zda se jedná o externě zajišťovaný systém IKT, a pokud ano, název poskytovatele služeb IKT z řad třetích stran;
         2. jurisdikce, v nichž se systém IKT používá;
         3. popis předběžného příznaku (předběžných příznaků) na vysoké úrovni s uvedením, ke kterému bezpečnostnímu aspektu důvěrnosti, integrity, autenticity nebo dostupnosti se každý příznak vztahuje.

PŘÍLOHA III

Obsah zprávy o cílených operativních informacích o hrozbách (čl. 10 odst. 5)

Zpráva o cílených operativních informacích o hrozbách obsahuje informace o všech následujících skutečnostech:

1. Celkový rozsah průzkumu operativních informací, který zahrnuje přinejmenším:
   a) zásadní nebo důležité funkce v rozsahu testování;
   b) jejich geografické umístění;
   c) používaný úřední jazyk EU;
   d) příslušné poskytovatele služeb IKT z řad třetích stran;
   e) časové období, za které je průzkum prováděn.
2. Celkové posouzení toho, jaké konkrétní využitelné operativní informace lze o finančním subjektu zjistit, včetně:
   a) uživatelských jmen a hesel zaměstnanců;
   b) vzhledově podobných domén, které mohou být zaměněny za oficiální domény finančního subjektu;
   c) technického průzkumu: zranitelný nebo zneužitelný software, systémy a technologie;
   d) informací zveřejněných zaměstnanci na internetu, které se týkají finančního subjektu a které by mohly být použity pro účely útoku;
   e) informací k prodeji na temném webu;
   f) veškerých dalších relevantních informací dostupných na internetu nebo veřejných sítích;
   g) případně informací o fyzickém zacílení, včetně způsobů přístupu do prostor finančního subjektu.
3. Analýza operativních informací o hrozbách s ohledem na obecné prostředí hrozeb a konkrétní situaci finančního subjektu, která zahrnuje přinejmenším:
   a) geopolitické prostředí;
   b) ekonomické prostředí;
   c) technologické trendy a další trendy související s činnostmi v odvětví finančních služeb.
4. Profily hrozeb ze strany zlovolných aktérů (konkrétní jednotlivec/skupina nebo obecná třída), kteří mohou cílit na finanční subjekt, včetně systémů finančního subjektu, které zlovolní aktéři s největší pravděpodobností ohrozí nebo na které se zaměří, možné motivace, záměru a odůvodnění potenciálního útoku a možného způsobu jednání útočníků.
5. Scénáře hrozeb: alespoň tři scénáře hrozeb mezi koncovými body pro profily hrozeb určené podle bodu 4, které vykazují nejvyšší skóre závažnosti hrozeb. Scénáře hrozeb popisují cestu útoku mezi koncovými body a zahrnují přinejmenším:
   a) jeden scénář, který zahrnuje mimo jiné narušení dostupnosti služeb;
   b) jeden scénář, který zahrnuje mimo jiné narušení integrity dat;
   c) jeden scénář, který zahrnuje mimo jiné narušení důvěrnosti informací.
6. Případně popis scénáře, který není založen na hrozbách, podle čl. 10 odst. 4.

PŘÍLOHA IV

Obsah plánu testování metodou „červeného týmu“ (čl. 11 odst. 1)

Plán testování metodou „červeného týmu“ obsahuje informace o všech následujících skutečnostech:

a) komunikační kanály a postupy;

b) taktiky, techniky a postupy povolené a nepovolené k použití při útoku, včetně etických hranic sociálního inženýrství;

c) opatření k řízení rizik, která mají subjekty provádějící testování dodržovat;

d) popis každého scénáře, včetně:

   i) simulovaného aktéra hrozby;

   ii) jeho záměrů, motivace a cílů;

   iii) cílové funkce (cílových funkcí) a podpůrného systému nebo podpůrných systémů IKT;

   iv) cílených aspektů důvěrnosti, integrity, dostupnosti a autenticity;

   v) příznaků;

e) podrobný popis každé předpokládané cesty útoku, včetně předběžných podmínek a možné podpory, kterou má řídící tým poskytnout, včetně lhůt pro její poskytnutí a možného využití;

f) časové rozvržení činností v rámci testování metodou „červeného týmu“, včetně časového plánování provedení jednotlivých scénářů, minimálně rozdělených podle tří fází, které subjekt provádějící testování v průběhu fáze testování absolvuje, resp. vstup do systémů IKT finančních subjektů, pohyb skrze systémy IKT a nakonec provedení akcí na cílech a nakonec opuštění systémů IKT (fáze „dovnitř“, „skrze“ a „ven“);

g) zvláštnosti infrastruktury finančních subjektů, které je třeba při testování zohlednit;

h) případné další informace nebo jiné zdroje, které subjekty provádějící testování potřebují k provedení scénářů.

PŘÍLOHA V

Obsah zprávy o testování metodou „červeného týmu“ (čl. 12 odst. 2)

Zpráva o testování metodou „červeného týmu“ musí obsahovat informace přinejmenším o všech následujících skutečnostech:

a) informace o provedeném útoku, včetně:

   i) cílových zásadních nebo důležitých funkcí a identifikovaných systémů, procesů a technologií IKT, které podporují zásadní nebo důležité funkce, jak je uvedeno v plánu testování metodou „červeného týmu“;

   ii) shrnutí jednotlivých scénářů;

   iii) dosažených a nedosažených příznaků;

   iv) úspěšně i neúspěšně sledovaných cest útoku;

   v) úspěšně i neúspěšně použitých taktik, technik a postupů;

   vi) případných odchylek od plánu testování metodou „červeného týmu“;

   vii) případně poskytnuté podpory;

b) všechny akce, o kterých subjekty provádějící testování vědí a které byly provedeny modrým týmem za účelem rekonstrukce útoku a zmírnění jeho následků;

c) objevené zranitelnosti a další zjištění, včetně:

   i) popisu zranitelností a dalších zjištění včetně jejich významu;

   ii) analýzy kořenových příčin úspěšných útoků;

   iii) doporučených nápravných opatření včetně uvedení priority nápravného opatření.

PŘÍLOHA VI

Obsah zprávy o testování metodou „modrého týmu“ (čl. 12 odst. 4)

Zpráva o testování metodou „modrého týmu“ musí obsahovat informace přinejmenším o všech následujících skutečnostech:

1. pro každý krok útoku popsaný subjekty provádějícími testování ve zprávě o testování metodou „červeného týmu“:
   a) seznam zjištěných akcí provedených v rámci útoku;
   b) záznamy protokolu odpovídající těmto zjištěným akcím;
2. vyhodnocení zjištění a doporučení subjektů provádějících testování;
3. důkazy o útoku subjektů provádějících testování shromážděné modrým týmem;
4. analýza kořenových příčin úspěšných útoků subjektů provádějících testování provedená modrým týmem;
5. seznam získaných zkušeností a zjištěných možností zlepšení;
6. seznam témat, která je třeba řešit v rámci fialového týmu.

PŘÍLOHA VII

Podrobnosti zprávy shrnující příslušná zjištění penetračního testování na základě hrozeb uvedené v čl. 26 odst. 6 nařízení (EU) 2022/2554

Souhrnná zpráva o testu musí obsahovat informace přinejmenším o všech následujících skutečnostech:

a) zúčastněné strany;

b) plán projektu;

c) ověřený rozsah, včetně odůvodnění zahrnutí nebo vyloučení zásadních nebo důležitých funkcí a identifikovaných systémů, procesů a technologií IKT, které podporují zásadní nebo důležité funkce, na něž se penetrační testování na základě hrozeb vztahuje;

d) vybrané scénáře a jakékoli významné odchylky od zprávy o cílených operativních informacích o hrozbách;

e) provedené cesty útoku a použité taktiky, techniky a postupy;

f) zachycené a nezachycené příznaky;

g) případné odchylky od plánu testování metodou „červeného týmu“;

h) případné detekce modrého týmu;

i) testování metodou „fialového týmu“ ve fázi testování, pokud se provádí, a související podmínky;

j) případně využitá podpora;

k) přijatá opatření k řízení rizik;

l) zjištěné zranitelnosti a další zjištění, včetně jejich významu;

m) analýza kořenových příčin úspěšných útoků;

n) plán nápravných opatření na vysoké úrovni, který propojí zranitelnosti a další zjištění, jejich kořenové příčiny a priority nápravných opatření;

o) zkušenosti získané z obdržené zpětné vazby.

PŘÍLOHA VIII

Podrobnosti osvědčení penetračního testování na základě hrozeb podle čl. 26 odst. 7 nařízení (EU) 2022/2554

Osvědčení obsahuje přinejmenším všechny tyto informace:

a) ohledně provedeného penetračního testování na základě hrozeb:

   i) datum zahájení a ukončení penetračního testování na základě hrozeb;

   ii) zásadní nebo důležité funkce spadající do rozsahu testu;

   iii) případné informace o zásadních nebo důležitých funkcích spadajících do rozsahu testu, ve vztahu k nimž penetrační testování na základě hrozeb nebylo provedeno;

   iv) případné další finanční subjekty, které se podílely na penetračním testování na základě hrozeb;

   v) případní poskytovatelé služeb IKT z řad třetích stran, kteří se účastnili penetračního testování na základě hrozeb;

   vi) ohledně subjektů provádějících testování:

      1. zda byly využity interní subjekty provádějící testování;

      2. zda finanční subjekt použil čl. 5 odst. 3 druhý pododstavec;

   vii) doba trvání fáze aktivního testování metodou „červeného týmu“ v kalendářních dnech;

b) v případě, že se na penetračním testování na základě hrozeb podílelo několik orgánů pro penetrační testování na základě hrozeb, další orgány pro penetrační testování na základě hrozeb a v jaké funkci;

c) seznam dokumentů, které orgán pro penetrační testování na základě hrozeb prověřil pro účely osvědčení.