Úřední věstník
Evropské unie

CS
Řada L

2024/1774

25.6.2024

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2024/1774

ze dne 13. března 2024,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující nástroje, metody, postupy a politiky řízení rizika v oblasti IKT a zjednodušený rámec pro řízení rizika v oblasti IKT

(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. 15 čtvrtý pododstavec a čl. 16 odst. 3 čtvrtý pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízení (EU) 2022/2554 se vztahuje na širokou škálu finančních subjektů, které se liší svou velikostí, strukturou, vnitřní organizací a povahou a složitostí svých činností, a vykazují tedy více či méně prvků složitosti nebo rizik. Aby byla jejich různorodost řádně zohledněna, měly by být veškeré požadavky na politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT a na zjednodušený rámec pro řízení rizika v oblasti IKT přiměřené velikosti, struktuře, vnitřní organizaci, povaze a složitosti těchto finančních subjektů a odpovídajícím rizikům.

(2) Ze stejného důvodu by finanční subjekty, na které se vztahuje nařízení (EU) 2022/2554, měly mít určitou flexibilitu, pokud jde o způsob, jakým plní veškeré požadavky na politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT, a pokud jde o jakýkoli zjednodušený rámec pro řízení rizika v oblasti IKT. Finanční subjekty by proto měly mít možnost použít ke splnění všech požadavků na dokumentaci, které z uvedených požadavků vyplývají, veškerou dokumentaci, kterou již mají k dispozici. Z toho vyplývá, že vypracování, dokumentace a provádění specifických politik v oblasti bezpečnosti IKT by měly být vyžadovány pouze pro určité zásadní prvky, mimo jiné s ohledem na osvědčené postupy a normy v odvětví. Pro zahrnutí specifických technických aspektů provádění je navíc nutné vypracovat, zdokumentovat a zavést postupy v oblasti bezpečnosti IKT, které budou pokrývat specifické technické aspekty provádění, včetně řízení kapacity a výkonu, řízení zranitelností a oprav, bezpečnosti údajů a systémů a vedení protokolů.

(3) Aby bylo v průběhu času zajištěno správné provádění politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v hlavě II kapitole I tohoto nařízení, je důležité, aby finanční subjekty správně přidělily a udržovaly všechny úlohy a povinnosti týkající se bezpečnosti IKT a aby stanovily důsledky nedodržení politik nebo postupů v oblasti bezpečnosti IKT.

(4) Pro účely zmírnění rizika střetu zájmů by finanční subjekty při přidělení úloh a povinností v oblasti IKT měly zajistit oddělení úkolů.

(5) V zájmu zajištění flexibility a zjednodušení kontrolního rámce finančních subjektů by se od finančních subjektů nemělo vyžadovat, aby vypracovávaly zvláštní ustanovení o důsledcích nedodržení politik, postupů a protokolů v oblasti bezpečnosti IKT uvedených v hlavě II kapitole I tohoto nařízení, pokud jsou tato ustanovení již stanovena v jiné politice nebo postupu.

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

(6) V dynamickém prostředí, v němž se rizika v oblasti IKT neustále vyvíjejí, je důležité, aby finanční subjekty vypracovaly svůj soubor politik v oblasti bezpečnosti IKT na základě osvědčených postupů a případně norem uvedených v čl. 2 bodě 1 nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([2]). To by mělo v měnícím se prostředí zajistit, aby finanční subjekty uvedené v hlavě II tohoto nařízení byly stále informované a připravené.

(7) Aby si finanční subjekty uvedené v hlavě II tohoto nařízení dokázaly zajistit svou digitální provozní odolnost, měly by v rámci svých politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT vypracovat a zavést politiku pro správu aktiv v oblasti IKT, postupy pro řízení kapacity a výkonu a politiky a postupy pro operace IKT. Tyto politiky a postupy jsou nezbytné k zajištění sledování stavu aktiv v oblasti IKT v průběhu jejich životního cyklu, aby byla tato aktiva efektivně využívána a udržována (správa aktiv v oblasti IKT). Tyto politiky a postupy by měly rovněž zajistit optimalizaci provozu systémů IKT a to, aby výkonnost systémů IKT a jejich kapacity odpovídala stanoveným obchodním cílům a cílům v oblasti bezpečnosti informací (řízení kapacity a výkonu). V neposlední řadě by tyto politiky a postupy měly zajistit účinnou a bezproblémovou každodenní správu a provoz systémů IKT (operace IKT), a tím minimalizovat riziko ztráty důvěrnosti, integrity a dostupnosti údajů. Tyto politiky a postupy jsou tedy nezbytné v zájmu zajištění bezpečnosti sítí, zavedení vhodných ochranných opatření proti vniknutí a zneužití údajů a zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů.

(8) Aby bylo zajištěno řádné řízení rizika původních systémů IKT, měly by finanční subjekty evidovat a sledovat dny ukončení služeb podpory IKT ze strany třetích stran. Vzhledem k tomu, že ztráta důvěrnosti, integrity a dostupnosti údajů může mít potenciální dopad, měly by se finanční subjekty při evidenci a sledování těchto dnů ukončení zaměřit na aktiva nebo systémy IKT, které jsou pro provoz podniku zásadní.

(9) Dostupnost, hodnověrnost, integritu a důvěrnost údajů mohou zajistit kryptografické kontroly. Finanční subjekty uvedené v hlavě II tohoto nařízení by proto měly tyto kontroly určit a zavést na základě přístupu založeného na riziku. Za tímto účelem by finanční subjekty měly dotčené údaje během jejich uchovávání, přenosu nebo v případě potřeby během jejich používání šifrovat na základě výsledků dvoustupňového procesu, a to klasifikace údajů a komplexního posouzení rizik v oblasti IKT. Vzhledem k tomu, že šifrování údajů během jejich používání je složité, měly by finanční subjekty uvedené v hlavě II tohoto nařízení šifrovat údaje během jejich používání pouze v případech, kdy by to bylo vhodné s ohledem na výsledky posouzení rizik v oblasti IKT. Pokud však šifrování údajů během jejich používání není proveditelné nebo je příliš složité, měly by finanční subjekty uvedené v hlavě II tohoto nařízení mít možnost zajistit důvěrnost, integritu a dostupnost dotčených údajů prostřednictvím jiných bezpečnostních opatření v oblasti IKT. Vzhledem k tomu, že v oblasti kryptografických technik dochází k rychlému technologickému vývoji, měly by finanční subjekty uvedené v hlavě II tohoto nařízení sledovat příslušný vývoj v oblasti kryptoanalýzy a zohledňovat osvědčené postupy a normy. Finanční subjekty uvedené v hlavě II tohoto nařízení by proto k tomu, aby se vypořádaly s dynamickým prostředím kryptografických hrozeb, včetně hrozeb vyplývajících z pokroku v oblasti kvantových technologií, měly uplatňovat flexibilní přístup založený na zmírňování a monitorování rizik.

(10) Pro zajištění důvěrnosti, integrity a dostupnosti údajů jsou nezbytné bezpečnost operací IKT a provozní politiky, postupy, protokoly a nástroje. Jedním z klíčových aspektů je přísné oddělení produkčních prostředí IKT od prostředí, v nichž se systémy IKT vyvíjejí a testují, nebo od jiných neprodukčních prostředí. Toto oddělení by mělo sloužit jako důležité bezpečnostní opatření v oblasti IKT, jež zabrání neúmyslnému a neoprávněnému přístupu k datům v produkčním prostředí, jejich změnám a vymazání, což by mohlo mít za následek závažné narušení obchodních operací finančních subjektů uvedených v hlavě II tohoto nařízení. S ohledem na současné postupy vývoje systémů IKT by však mělo být finančním subjektům ve výjimečných případech umožněno testovat i v produkčním prostředí, pokud toto testování odůvodní a získají k němu potřebný souhlas.

([2]) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Rychle se měnící charakter prostředí IKT, zranitelnosti IKT a kybernetických hrozeb vyžaduje, aby byl k identifikaci, hodnocení a řešení zranitelností IKT přijat proaktivní a komplexní přístup. Bez přijetí tohoto přístupu mohou být finanční subjekty, jejich zákazníci, uživatelé nebo protistrany vystaveni vážným rizikům, která by ohrozila jejich digitální provozní odolnost, bezpečnost jejich sítí a dostupnost, hodnověrnost, integritu a důvěrnost údajů, jejichž ochranu by měly politiky a postupy v oblasti bezpečnosti IKT zajišťovat. Finanční subjekty uvedené v hlavě II tohoto nařízení by proto měly identifikovat a odstraňovat zranitelnosti ve svém prostředí IKT a ony samy i jejich poskytovatelé služeb IKT z řad třetích stran by měli dodržovat ucelený, transparentní a odpovědný rámec pro řízení zranitelností. Ze stejného důvodu by finanční subjekty měly sledovat zranitelnosti v oblasti IKT za použití spolehlivých zdrojů a automatizovaných nástrojů a ověřovat, zda poskytovatelé služeb IKT z řad třetích stran provádějí v případě, že zjistí zranitelnosti poskytovaných služeb IKT, urychlená opatření.

(12) Řízení oprav by mělo být klíčovou součástí těch politik a postupů v oblasti bezpečnosti IKT, které mají prostřednictvím testování a využívání v kontrolovaném prostředí vyřešit zjištěné zranitelnosti a zabránit narušením provozu v důsledku instalace oprav.

(13) Aby bylo zajištěno včasné a transparentní informování o potenciálních bezpečnostních hrozbách, které by mohly mít dopad na finanční subjekt a jeho zúčastněné strany, měly by finanční subjekty zavést postupy pro odpovědné informování klientů, protistran a veřejnosti o zranitelnostech v oblasti IKT. Při stanovování těchto postupů by finanční subjekty měly zvážit faktory, jako je závažnost zranitelnosti, potenciální dopad této zranitelnosti na zúčastněné strany a připravenost k přijetí nápravných nebo zmírňujících opatření.

(14) Aby mohly přidělovat uživatelská přístupová práva, měly by finanční subjekty uvedené v hlavě II tohoto nařízení zavést silná opatření k zjištění jedinečné identifikace osob a systémů, které budou mít přístup k informacím finančního subjektu. Pokud by tak finanční subjekty neučinily, byly by vystaveny možnému neoprávněnému přístupu, prolomení důvěrných údajů a podvodnému jednání, čímž by byla ohrožena důvěrnost, integrita a dostupnost citlivých finančních údajů. Používání obecných nebo sdílených účtů by mělo být povoleno pouze ve výjimečných případech, a to za podmínek stanovených finančními subjekty. Finanční subjekty by však měly zajistit, aby byla zachována odpovědnost za činnosti prováděné prostřednictvím těchto účtů. Bez této záruky by případní škodliví uživatelé mohli bránit provádění opatření při vyšetřování a nápravných opatření, což by finanční subjekty mohlo učinit zranitelnými vůči skrytým škodlivým aktivitám nebo je vystavit riziku udělení sankcí za nedodržení předpisů.

(15) Aby se finanční subjekty uvedené v hlavě II tohoto nařízení dokázaly přizpůsobit rychlému vývoji v prostředí IKT, měly by zavést spolehlivé politiky a postupy pro řízení projektů v oblasti IKT, a zajistit tak dostupnost, hodnověrnost, integritu a důvěrnost údajů. Tyto politiky a postupy pro řízení projektů v oblasti IKT by měly identifikovat prvky, které jsou nezbytné pro úspěšné řízení projektů v oblasti IKT, včetně změn, pořízení, údržby a rozvoje systémů IKT finančního subjektu, a to bez ohledu na metodiku řízení projektů v oblasti IKT, kterou finanční subjekt zvolil. V souvislosti s těmito politikami a postupy by finanční subjekty měly přijmout testovací postupy a metody, které odpovídají jejich potřebám, a zároveň dodržovat přístup založený na posouzení rizik a zajišťovat, aby bylo zachováno bezpečné, spolehlivé a odolné prostředí IKT. Aby byla zaručena bezpečná realizace projektu v oblasti IKT, měly by finanční subjekty zajistit, aby zaměstnanci určitých provozních oblastí nebo s určitými úlohami, které daný projekt v oblasti IKT ovlivňuje nebo na ně má dopad, poskytli potřebné informace a odborné znalosti. Pro zajištění účinného dohledu by měly být vedoucímu orgánu předkládány zprávy o projektech v oblasti IKT, zejména o projektech, které mají vliv na zásadní nebo důležité funkce, a o souvisejících rizicích. Finanční subjekty by měly přizpůsobit četnost a míru podrobnosti systematických a průběžných přezkumů a zpráv významu a velikosti příslušných projektů v oblasti IKT.

(16) Je nezbytné zajistit, aby softwarové balíčky, které finanční subjekty uvedené v hlavě II tohoto nařízení pořizují a vyvíjejí, byly účinně a bezpečně integrovány do stávajícího prostředí IKT, a to v souladu se stanovenými provozními cíli a cíli v oblasti bezpečnosti informací. Finanční subjekty by proto měly tyto softwarové balíčky důkladně posoudit. Za tímto účelem a za účelem identifikace zranitelností a potenciálních bezpečnostních nedostatků v případě softwarových balíčků i širších systémů IKT by finanční subjekty měly provádět testování bezpečnosti IKT. Aby bylo možné posoudit integritu softwaru a zajistit, že používání tohoto softwaru nepředstavuje bezpečnostní riziko pro IKT, měly by finanční subjekty rovněž prověřit zdrojové kódy pořízeného softwaru, včetně proprietárního softwaru poskytnutého poskytovateli služeb IKT z řad třetích stran, je-li to možné, a to pomocí metod statického i dynamického testování.

(17) Změny s sebou bez ohledu na svůj rozsah přirozeně nesou rizika a mohou představovat i významná rizika ztráty důvěrnosti, integrity a dostupnosti údajů, což může způsobit závažná narušení provozu. Aby byly finanční subjekty chráněny před možnými zranitelnostmi a slabými místy v oblasti IKT, které by je mohly vystavit významným rizikům, je nutné provést důsledné ověření, které potvrdí, že všechny změny splňují nezbytné požadavky na bezpečnost IKT. Finanční subjekty uvedené v hlavě II tohoto nařízení by proto měly mít jako základní prvek svých politik a postupů v oblasti bezpečnosti IKT zavedeny spolehlivé politiky a postupy pro řízení změn v oblasti IKT. Aby byla zajištěna objektivita a účinnost procesu řízení změn v oblasti IKT a zabránilo se střetům zájmů a zajistilo se objektivní hodnocení změn v oblasti IKT, je nutné oddělit funkce, jež jsou odpovědné za schvalování těchto změn, od funkcí, které o tyto změny žádají a které je provádějí. Aby bylo dosaženo účinných přechodů, řízeného provádění změn v oblasti IKT a minimálního narušení provozu systémů IKT, měly by finanční subjekty přidělit jasné úlohy a povinnosti, které zajistí, že změny v oblasti IKT budou plánovány, náležitě testovány a že bude zajištěna jejich kvalita. Pro zajištění toho, aby systémy IKT i nadále účinně fungovaly a aby finanční subjekty měly k dispozici záchrannou síť, by finanční subjekty měly rovněž vypracovat a zavést záložní postupy. Finanční subjekty by měly tyto záložní postupy jasně určit a přidělit povinnosti, aby byla zajištěna rychlá a účinná reakce v případě neúspěšných změn v oblasti IKT.

(18) Za účelem detekce, řízení a hlášení incidentů souvisejících s IKT by finanční subjekty uvedené v hlavě II tohoto nařízení měly zavést politiku pro incidenty související s IKT, která by zahrnovala součásti procesu řízení incidentů souvisejících s IKT. Za tímto účelem by finanční subjekty měly určit všechny relevantní kontakty uvnitř organizace i mimo ni, které mohou usnadnit správnou koordinaci a realizaci jednotlivých fází tohoto procesu. V zájmu optimalizace detekce incidentů souvisejících s IKT a reakce na ně a v zájmu identifikace trendů u těchto incidentů, které jsou cenným zdrojem informací umožňujících finančním subjektům identifikovat a účinně řešit hlavní příčiny a problémy, by finanční subjekty měly zejména podrobně analyzovat incidenty související s IKT, které považují za nejvýznamnější, mimo jiné z toho důvodu, že se pravidelně opakují.

(19) Aby byla zaručena včasná a účinná detekce neobvyklých aktivit, měly by finanční subjekty uvedené v hlavě II tohoto nařízení shromažďovat, monitorovat a analyzovat různé zdroje informací a měly by přidělit související úlohy a povinnosti. Co se týče interních zdrojů informací, jsou mimořádně důležitým zdrojem protokoly, nicméně finanční subjekty by se neměly spoléhat pouze na protokoly. Místo toho by se finanční subjekty měly spoléhat i na informace hlášené jinými interními funkcemi, protože tyto funkce jsou mnohdy cenným zdrojem relevantních informací. Ze stejného důvodu by finanční subjekty měly analyzovat a sledovat informace získané z externích zdrojů, včetně informací poskytovaných poskytovateli služeb IKT z řad třetích stran o incidentech, které mají dopad na jejich systémy a sítě, a dalších zdrojů informací, které finanční subjekty považují za relevantní. Pokud jsou tyto informace ve formě osobních údajů, použijí se právní předpisy Unie o ochraně údajů. Osobní údaje by měly být omezeny na to, co je nezbytné pro detekci incidentů.

(20) Pro usnadnění detekce incidentů souvisejících s IKT by měly finanční subjekty uchovávat důkazy o těchto incidentech. Aby se na jedné straně zajistilo, že tyto důkazy budou uchovávány dostatečně dlouhou dobu, a na druhé straně se zabránilo nadměrné regulační zátěži, měly by finanční subjekty stanovit dobu uchovávání mimo jiné s ohledem na význam údajů a požadavky na uchovávání, které vyplývají z práva Unie.

(21) Aby byla zajištěna včasná detekce incidentů souvisejících s IKT, neměly by finanční subjekty uvedené v hlavě II tohoto nařízení považovat kritéria stanovená pro zahájení detekce incidentů souvisejících s IKT a reakce na ně za vyčerpávající. Ačkoli by finanční subjekty měly zvážit každé z těchto kritérií, okolnosti popsané v kritériích by navíc nemusely nastat současně a pro spuštění procesů detekce incidentů souvisejících s IKT a reakce na ně by měla být vhodným způsobem zvážena důležitost dotčených služeb IKT.

(22) Při vypracovávání politiky zachování provozu IKT by finanční subjekty uvedené v hlavě II tohoto nařízení měly zohlednit základní složky řízení rizik v oblasti IKT, včetně strategie řízení incidentů souvisejících s IKT a komunikační strategie, procesu řízení změn v oblasti IKT a rizik spojených s poskytovateli služeb IKT z řad třetích stran.

(23) Je nezbytné stanovit soubor scénářů, které by finanční subjekty uvedené v hlavě II tohoto nařízení měly zohlednit jak při provádění plánů reakce a obnovy v oblasti IKT, tak při testování plánů zachování provozu IKT. Tyto scénáře by měly sloužit finančním subjektům jako výchozí bod pro analýzu významu a věrohodnosti jednotlivých scénářů a potřeby vypracovat alternativní scénáře. Finanční subjekty by se měly zaměřit na ty scénáře, v nichž by investice do opatření na zvýšení odolnosti mohly být účinnější a účelnější. Na základě testování přechodu z primární infrastruktury IKT na jakoukoli rezervní kapacitu, záložní a rezervní zařízení by finanční instituce měly posoudit, zda tato kapacita, zálohy a zařízení fungují efektivně po dostatečně dlouhou dobu, a zajistit, aby bylo obnoveno normální fungování primární infrastruktury IKT v souladu s cíli pro obnovu.

(24) Je nezbytné stanovit požadavky na operační riziko, a zejména požadavky na řízení projektů a změn v oblasti IKT a na řízení zachování provozu IKT, v návaznosti na požadavky, které se již vztahují na ústřední protistrany, centrální depozitáře cenných papírů a obchodní systémy podle nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ([3]), (EU) č. 600/2014 ([4]) a (EU) č. 909/2014 ([5]).

(25) Ustanovení čl. 6 odst. 5 nařízení (EU) 2022/2554 vyžaduje, aby finanční subjekty přezkoumaly svůj rámec pro řízení rizika v oblasti IKT a předložily příslušnému orgánu zprávu o tomto přezkumu. Aby mohly příslušné orgány snadno zpracovávat informace obsažené v těchto zprávách a aby bylo zaručeno odpovídající předávání těchto informací, měly by finanční subjekty předkládat tyto zprávy v elektronickém formátu, který umožňuje vyhledávání.

(26) Požadavky na finanční subjekty, na které se vztahuje zjednodušený rámec pro řízení rizika v oblasti IKT uvedený v článku 16 nařízení (EU) 2022/2554, by se měly zaměřit na ty základní oblasti a prvky, které jsou s ohledem na rozsah, rizika, velikost a složitost těchto finančních subjektů nezbytné alespoň k zajištění důvěrnosti, integrity, dostupnosti a hodnověrnosti údajů a služeb těchto finančních subjektů. V této souvislosti by tyto finanční subjekty měly mít zaveden interní řídicí a kontrolní rámec s jasnými povinnostmi, který by umožňoval účinné a řádné řízení rizik. Kromě toho by tyto finanční subjekty měly v zájmu snížení administrativní a provozní zátěže vypracovat a zdokumentovat pouze jednu politiku, a to politiku bezpečnosti informací, která stanoví zásady a pravidla na vysoké úrovni nezbytná pro zajištění důvěrnosti, integrity, dostupnosti a hodnověrnosti údajů a služeb těchto finančních subjektů.

(27) Ustanovení tohoto nařízení se týkají rámce pro řízení rizika v oblasti IKT, a to tak, že podrobně popisují konkrétní prvky použitelné na finanční subjekty v souladu s článkem 15 nařízení (EU) 2022/2554 a navrhují zjednodušený rámec pro řízení rizika v oblasti IKT pro finanční subjekty stanovené v čl. 16 odst. 1 uvedeného nařízení. V zájmu zajištění soudržnosti mezi běžným a zjednodušeným rámcem pro řízení rizika v oblasti IKT a vzhledem k tomu, že by tato ustanovení měla být použitelná současně, je vhodné zahrnout tato ustanovení do jednoho legislativního aktu.

(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 („evropskými orgány dohledu“), a to po konzultaci s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA).

([3]) Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (Úř. věst. L 201, 27.7.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) 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).

([5]) Nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ze dne 23. července 2014 o zlepšení vypořádání obchodů s cennými papíry v Evropské unii a centrálních depozitářích cenných papírů a o změně směrnic 98/26/ES a 2014/65/EU a nařízení (EU) č. 236/2012 (Úř. věst. L 257, 28.8.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Společný výbor evropských orgánů dohledu uvedený v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([6]), v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ([7]) a v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ([8]) provedl k návrhům regulačních technických norem, z nichž toto nařízení vychází, otevřené veřejné konzultace, analyzoval potenciální náklady a přínosy navrhovaných norem a vyžádal si stanovisko skupiny subjektů působících v bankovnictví zřízené podle článku 37 nařízení (EU) č. 1093/2010, skupiny subjektů působících v oblasti pojištění a zajištění a skupiny subjektů působících v oblasti zaměstnaneckého penzijního pojištění zřízených podle článku 37 nařízení (EU) č. 1094/2010 a skupiny subjektů působících v oblasti cenných papírů a trhů zřízené podle článku 37 nařízení (EU) č. 1095/2010.

(30) V rozsahu, v jakém je pro splnění povinností stanovených tímto aktem vyžadováno zpracování osobních údajů, by se mělo plně použít nařízení Evropského parlamentu a Rady (EU) 2016/679 ([9]) a nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([10]). Například v případě shromažďování osobních údajů pro účely řádné detekce incidentů by měla být dodržována zásada minimalizace údajů. Návrh znění tohoto aktu byl konzultován také s evropským inspektorem ochrany údajů,

PŘIJALA TOTO NAŘÍZENÍ:

HLAVA I

OBECNÁ ZÁSADA

Článek 1

Celkový rizikový profil a složitost

Při vypracovávání a provádění politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v hlavě II a zjednodušeného rámce pro řízení rizika v oblasti IKT uvedeného v hlavě III se zohlední velikost a celkový rizikový profil finančního subjektu a povaha, rozsah a prvky zvýšené nebo snížené složitosti jeho služeb, činností a operací, včetně prvků týkajících se:

a) šifrování a kryptografie;

b) bezpečnosti operací IKT;

c) bezpečnosti sítí;

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) 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, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) řízení projektů a změn v oblasti IKT;

e) potenciálního dopadu rizika v oblasti IKT na důvěrnost, integritu a dostupnost údajů a potenciálního dopadu narušení na zachování provozu a dostupnosti činností finančního subjektu.

HLAVA II

DALŠÍ HARMONIZACE NÁSTROJŮ, METOD, POSTUPŮ A POLITIK ŘÍZENÍ RIZIKA V OBLASTI IKT V SOULADU S ČLÁNKEM 15 NAŘÍZENÍ (EU) 2022/2554

KAPITOLA I

Politiky, postupy, protokoly a nástroje v oblasti bezpečnosti ikt

Oddíl 1

Článek 2

Obecné prvky politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT

1. Finanční subjekty zajistí, aby do jejich rámce pro řízení rizika v oblasti IKT byly začleněny jejich politiky v oblasti bezpečnosti IKT, bezpečnosti informací a související postupy, protokoly a nástroje uvedené v čl. 9 odst. 2 nařízení (EU) 2022/2554. Finanční subjekty zavedou politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT stanovené v této kapitole, které:

a) zajistí bezpečnost sítí;

b) obsahují ochranná opatření proti vniknutí a zneužití údajů;

c) zachovají dostupnost, hodnověrnost, integritu a důvěrnost údajů, a to i prostřednictvím kryptografických technik;

d) zaručí přesný a rychlý přenos dat bez vážných narušení a zbytečných prodlev.

2. Finanční subjekty zajistí, aby politiky v oblasti bezpečnosti IKT uvedené v odstavci 1:

a) byly v souladu s cíli finančního subjektu v oblasti bezpečnosti informací, které jsou zahrnuty do strategie digitální provozní odolnosti uvedené v čl. 6 odst. 8 nařízení (EU) 2022/2554;

b) uváděly datum formálního schválení politik v oblasti bezpečnosti IKT vedoucím orgánem;

c) obsahovaly ukazatele a opatření:

   i) ke sledování provádění politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT;

   ii) k zaznamenání výjimek z tohoto provádění;

   iii) k zaručení toho, aby v případě výjimek uvedených v bodě ii) byla zajištěna digitální provozní odolnost finančního subjektu;

d) specifikovaly povinnosti zaměstnanců na všech úrovních při zajišťování bezpečnosti IKT finančního subjektu;

e) specifikovaly důsledky nedodržování politik v oblasti bezpečnosti IKT zaměstnanci finančního subjektu, pokud tato ustanovení nejsou stanovena v jiných politikách finančního subjektu;

f) uváděly seznam dokumentace, která má být vedena;

g) specifikovaly opatření pro oddělení úkolů v kontextu modelu tří linií obrany nebo jiného interního modelu řízení a kontroly rizika, aby se předešlo střetu zájmů;

h) braly v potaz osvědčené postupy a případně normy vymezené v čl. 2 bodě 1 nařízení (EU) č. 1025/2012;

i) určily úlohy a odpovědnost za vývoj, provádění a udržování politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT;

j) byly přezkoumávány podle čl. 6 odst. 5 nařízení (EU) 2022/2554;

k) zohledňovaly podstatné změny týkající se finančního subjektu, včetně podstatných změn činností nebo procesů finančního subjektu, prostředí kybernetických hrozeb nebo platných právních povinností.

Oddíl 2

Článek 3

Řízení rizika v oblasti IKT

Finanční subjekty vypracují, zdokumentují a zavedou politiky a postupy pro řízení rizika v oblasti IKT, které obsahují všechny následující prvky:

a) údaj o schválení přípustné odchylky rizika v oblasti IKT stanovené v souladu s čl. 6 odst. 8 písm. b) nařízení (EU) 2022/2554;

b) postup a metodika pro provádění posouzení rizika v oblasti IKT, přičemž se určí:

   i) zranitelnosti a hrozby, které ovlivňují nebo mohou ovlivnit podporované obchodní funkce, systémy IKT a aktiva v oblasti IKT podporující tyto funkce;

   ii) kvantitativní nebo kvalitativní ukazatele pro měření dopadu a pravděpodobnosti zranitelností a hrozeb uvedených v bodě i);

c) postup pro určení, zavedení a zdokumentování opatření k řešení rizik v oblasti IKT pro zjištěná a posouzená rizika v oblasti IKT, včetně stanovení opatření k řešení rizik v oblasti IKT nezbytných k tomu, aby se riziko v oblasti IKT dostalo do rozmezí přípustné odchylky rizika uvedené v písmenu a);

d) pro zbytková rizika v oblasti IKT, která po provedení opatření k řešení rizik v oblasti IKT uvedených v písmenu c) stále existují:

   i) ustanovení o identifikaci těchto zbytkových rizik v oblasti IKT;

   ii) přidělení úloh a povinností týkajících se:

      1) přijetí zbytkových rizik v oblasti IKT, která přesahují přípustnou odchylku rizika finančního subjektu uvedenou v písmenu a),

      2) procesu přezkumu uvedeného v tomto písm. d) bodě iv);

   iii) vypracování soupisu přijatých zbytkových rizik v oblasti IKT, včetně odůvodnění jejich přijetí;

   iv) ustanovení o přezkumu přijatých zbytkových rizik v oblasti IKT alespoň jednou ročně, včetně:

      1) identifikace jakýchkoli změn zbytkových rizik v oblasti IKT,

      2) posouzení dostupných zmírňujících opatření,

      3) posouzení, zda důvody pro přijetí zbytkových rizik v oblasti IKT jsou ke dni přezkumu stále platné a použitelné;

e) ustanovení o sledování:

   i) veškerých změn rizik v oblasti IKT a prostředí kybernetických hrozeb;

   ii) vnitřních a vnějších zranitelností a hrozeb;

   iii) rizika finančního subjektu v oblasti IKT, které umožňuje rychlou detekci změn, jež by mohly ovlivnit jeho rizikový profil v oblasti IKT;

f) ustanovení ohledně procesu, který zajistí, aby byly zohledněny veškeré změny obchodní strategie a strategie digitální provozní odolnosti finančního subjektu.

Pro účely prvního pododstavce písm. c) se postupem podle uvedeného písmene zajistí:

a) sledování účinnosti zavedených opatření k řešení rizik v oblasti IKT;

b) posouzení, zda bylo dosaženo stanovených úrovní přípustné odchylky rizika finančního subjektu;

c) posouzení, zda finanční subjekt v případě potřeby přijal opatření k nápravě nebo zlepšení těchto opatření.

Oddíl 3

Správa aktiv v oblasti ikt

Článek 4

Politika správy aktiv v oblasti IKT

1. V rámci politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou politiku správy aktiv v oblasti IKT.

2. Politika správy aktiv v oblasti IKT uvedená v odstavci 1:

a) stanoví sledování a řízení životního cyklu aktiv v oblasti IKT identifikovaných a klasifikovaných v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554;

b) stanoví, aby finanční subjekt vedl záznamy o všech následujících skutečnostech:

   i) jedinečný identifikátor každého aktiva v oblasti IKT;

   ii) informace o fyzickém nebo logickém umístění všech aktiv v oblasti IKT;

   iii) klasifikace všech aktiv v oblasti IKT ve smyslu čl. 8 odst. 1 nařízení (EU) 2022/2254;

   iv) totožnost vlastníků aktiv v oblasti IKT;

   v) obchodní funkce nebo služby podporované daným aktivem v oblasti IKT;

   vi) požadavky na zachování provozu IKT, včetně cílů, pokud jde o dobu obnovy a bod dosažení obnovy;

   vii) zda aktivum v oblasti IKT může být nebo je vystaveno vnějším sítím, včetně internetu;

   viii) vazby a vzájemné závislosti mezi aktivy v oblasti IKT a obchodními funkcemi využívajícími jednotlivá aktiva v oblasti IKT;

   ix) v příslušných případech pro všechna aktiva v oblasti IKT data ukončení poskytování pravidelných, rozšířených a přizpůsobených služeb podpory poskytovaných poskytovatelem služeb IKT z řad třetích stran, po jejichž uplynutí již tato aktiva v oblasti IKT nejsou jejich dodavatelem nebo poskytovatelem služeb IKT z řad třetích stran podporována;

c) pro finanční subjekty jiné než mikropodniky stanoví, aby tyto finanční subjekty vedly záznamy o informacích nezbytných k provedení zvláštního posouzení rizik v oblasti IKT u všech původních systémů IKT ve smyslu čl. 8 odst. 7 nařízení (EU) 2022/2554.

Článek 5

Postup pro správu aktiv v oblasti IKT

1. Finanční subjekty vypracují, zdokumentují a zavedou postup pro správu aktiv v oblasti IKT.

2. Postup pro správu aktiv v oblasti IKT uvedený v odstavci 1 stanoví kritéria pro provedení posouzení kritičnosti informačních aktiv a aktiv v oblasti IKT podporujících obchodní funkce. Při tomto posouzení se zohlední:

a) rizika v oblasti IKT související s těmito obchodními funkcemi a jejich závislost na informačních aktivech nebo aktivech v oblasti IKT;

b) to, jak by ztráta důvěrnosti, integrity a dostupnosti těchto informačních aktiv a aktiv v oblasti IKT ovlivnila obchodní procesy a činnosti finančních subjektů.

Oddíl 4

Šifrování a kryptografie

Článek 6

Šifrování a kryptografické kontroly

1. V rámci svých politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou politiku šifrování a kryptografických kontrol.

2. Finanční subjekty navrhnou politiku šifrování a kryptografických kontrol uvedenou v odstavci 1 na základě výsledků schválené klasifikace dat a posuzování rizika v oblasti IKT. Tato politika obsahuje pravidla pro všechny následující oblasti:

a) šifrování údajů během jejich uchovávání a přenosu;

b) v případě potřeby šifrování údajů během jejich používání;

c) šifrování interních síťových připojení a provozu s externími stranami;

d) správa kryptografických klíčů uvedená v článku 7, v jejímž rámci jsou stanovena pravidla pro správné používání, ochranu a životní cyklus kryptografických klíčů.

Pro účely písmene b), pokud šifrování údajů během jejich používání není možné, zpracovávají finanční subjekty údaje během jejich používání v odděleném a chráněném prostředí nebo přijmou rovnocenná opatření k zajištění důvěrnosti, integrity, hodnověrnosti a dostupnosti údajů.

3. Finanční subjekty zahrnou do politiky šifrování a kryptografických kontrol uvedené v odstavci 1 kritéria pro výběr kryptografických technik a postupy jejich používání s přihlédnutím k osvědčeným postupům a normám podle čl. 2 bodu 1 nařízení (EU) č. 1025/2012 a ke klasifikaci příslušných aktiv v oblasti IKT stanovené v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554. Finanční subjekty, které nejsou schopny dodržovat osvědčené postupy či normy nebo používat nejspolehlivější techniky, musí přijmout opatření ke zmírnění a monitorování, která zajistí odolnost vůči kybernetickým hrozbám.

4. Finanční subjekty zahrnou do politiky šifrování a kryptografických kontrol uvedené v odstavci 1 ustanovení o případné aktualizaci nebo změně kryptografické technologie na základě vývoje v oblasti kryptoanalýzy. Tyto aktualizace nebo změny zajistí, aby kryptografická technologie zůstala odolná vůči kybernetickým hrozbám, jak požaduje čl. 10 odst. 2 písm. a). Finanční subjekty, které nejsou schopny aktualizovat nebo změnit kryptografickou technologii, přijmou opatření ke zmírnění a monitorování, která zajistí odolnost proti kybernetickým hrozbám.

5. Finanční subjekty zahrnou do politiky šifrování a kryptografických kontrol uvedené v odstavci 1 požadavek na vedení záznamů o přijetí opatření ke zmírnění a sledování přijatých v souladu s odstavci 3 a 4 s uvedením důvodů, proč tak učinily.

Článek 7

Správa kryptografických klíčů

1. Finanční subjekty zahrnou do politiky správy kryptografických klíčů uvedené v čl. 6 odst. 2 písm. d) požadavky na správu kryptografických klíčů v průběhu celého jejich životního cyklu, včetně generování, obnovování, ukládání, zálohování, archivace, vyhledávání, předávání, vyřazování, odvolávání a likvidace těchto kryptografických klíčů.

2. Finanční subjekty určí a zavedou kontrolní mechanismy na ochranu kryptografických klíčů během celého jejich životního cyklu před ztrátou, neoprávněným přístupem, zveřejněním a modifikací. Finanční subjekty navrhnou tyto kontrolní mechanismy na základě výsledků schválené klasifikace dat a posuzování rizika v oblasti IKT.

3. Finanční subjekty vypracují a zavedou metody pro nahrazování kryptografických klíčů v případě jejich ztráty nebo v případě, že jsou tyto klíče narušeny či poškozeny.

4. Finanční subjekty vytvoří a vedou registr všech certifikátů a zařízení pro uchovávání certifikátů alespoň pro aktiva v oblasti IKT, jež podporují zásadní nebo důležité funkce. Tento registr finanční subjekty pravidelně aktualizují.

5. Finanční subjekty zajistí včasné obnovení certifikátů před uplynutím doby jejich platnosti.

Oddíl 5

Bezpečnost operací ikt

Článek 8

Politiky a postupy pro operace IKT

1. V rámci politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou politiky a postupy pro řízení operací IKT. Tyto politiky a postupy stanoví, jak finanční subjekty provozují, monitorují, kontrolují a obnovují svá aktiva v oblasti IKT, včetně dokumentace operací IKT.

2. Politiky a postupy pro operace IKT uvedené v odstavci 1 obsahují všechny tyto prvky:

a) popis aktiv v oblasti IKT, včetně všech následujících údajů:

   i) požadavky na bezpečnou instalaci, údržbu, konfiguraci a deinstalaci systému IKT;

   ii) požadavky týkající se správy informačních aktiv využívaných aktivy v oblasti IKT, včetně jejich zpracování a jejich používání, a to jak automatizovaného, tak manuálního;

   iii) požadavky týkající se identifikace a kontroly původních systémů IKT;

b) kontroly a monitorování systémů IKT, včetně všech následujících položek:

   i) požadavky na zálohování a obnovu systémů IKT;

   ii) požadavky na časové plánování s ohledem na vzájemné závislosti mezi systémy IKT;

   iii) protokoly pro auditní stopu a informace systémového protokolu;

   iv) požadavky na zajištění toho, aby provádění interního auditu a dalších testů co nejméně narušovalo obchodní činnost;

   v) požadavky na oddělení produkčních prostředí IKT od vývojových, testovacích a jiných neprodukčních prostředí;

   vi) požadavky na provádění vývoje a testování v prostředích, která jsou oddělena od produkčního prostředí;

   vii) požadavky na provádění vývoje a testování v produkčním prostředí;

c) řešení chyb systémů IKT, včetně všech následujících položek:

i) postupy a protokoly pro řešení chyb;

ii) kontakty pro účely podpory a eskalace, včetně kontaktů na externí podporu v případě neočekávaných provozních nebo technických problémů;

iii) postupy pro restartování, zpětné obnovení („rollback“) a obnovu systému IKT, které se použijí v případě narušení systému IKT.

Pro účely písm. b) bodu v) se oddělení týká všech složek prostředí, včetně účtů, dat nebo spojení, jak požaduje čl. 13 první podostavec písm. a).

Pro účely písmene b) bodu vii) musí politiky a postupy uvedené v odstavci 1 stanovit, že případy, kdy je testování prováděno v produkčním prostředí, jsou jasně stanoveny, odůvodněny, jsou časově omezené a jsou schváleny příslušnou funkcí v souladu s čl. 16 odst. 6. Během vývojových a testovacích činností v produkčním prostředí finanční subjekty zajistí dostupnost, důvěrnost, integritu a hodnověrnost systémů IKT a produkčních dat.

Článek 9

Řízení kapacity a výkonu

1. V rámci politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou postupy řízení kapacity a výkonu za účelem:

a) identifikace požadavků na kapacitu svých systémů IKT;

b) uplatnění optimalizace zdrojů;

c) monitoringu pro zachování a zlepšování:

i) dostupnosti údajů a systémů IKT;

ii) účinnosti systémů IKT;

iii) předcházení nedostatku kapacity IKT.

2. Postupy řízení kapacity a výkonu uvedené v odstavci 1 zajistí, aby finanční subjekty přijaly opatření, která jsou vhodná pro zohlednění specifik systémů IKT s dlouhými nebo složitými procesy pořízení nebo schvalování nebo systémů IKT náročných na zdroje.

Článek 10

Řízení zranitelností a oprav

1. V rámci politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou postupy řízení zranitelností.

2. Postupy řízení zranitelností uvedené v odstavci 1:

a) identifikují a aktualizují relevantní a důvěryhodné informační zdroje, aby bylo možné vytvořit a udržovat povědomí o zranitelnostech;

b) zajišťují provádění automatizovaného skenování a posuzování zranitelností aktiv v oblasti IKT, přičemž četnost a rozsah těchto činností musí být úměrné klasifikaci stanovené v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554 a celkovému rizikovému profilu aktiva v oblasti IKT;

c) ověřují, zda:

i) poskytovatelé služeb IKT z řad třetích stran řeší zranitelnosti související se službami IKT poskytovanými finančnímu subjektu;

ii) zda tito poskytovatelé služeb finančnímu subjektu včas hlásí alespoň kritické zranitelnosti a statistiky a trendy;

d) sledují používání:

i) knihoven třetích stran, včetně knihoven s otevřeným zdrojovým kódem, které používají služby IKT podporující zásadní nebo důležité funkce;

ii) služeb IKT vyvinutých samotným finančním subjektem nebo speciálně přizpůsobených či vyvinutých pro finanční subjekt poskytovatelem služeb IKT z řad třetích stran;

e) stanoví postupy pro odpovědné informování klientů, protistran a veřejnosti o zranitelnostech;

f) stanoví priority pro zavádění oprav a dalších opatření ke zmírnění zjištěných zranitelností;

g) sledují a ověřují nápravu zranitelností;

h) vyžadují evidenci všech zjištěných zranitelností, jež mají dopad na systémy IKT, a sledování jejich řešení.

Pro účely písmene b) u aktiv v oblasti IKT podporujících zásadní nebo důležité funkce provádějí finanční subjekty automatizované skenování a posuzování zranitelností alespoň jednou týdně.

Pro účely písmene c) finanční subjekty požádají poskytovatele služeb IKT z řad třetích stran, aby prošetřili příslušné zranitelnosti, určili jejich hlavní příčiny a provedli příslušná zmírňující opatření.

Pro účely písmene d) finanční subjekty, případně ve spolupráci s poskytovatelem služeb IKT z řad třetích stran, sledují verzi a případné aktualizace knihoven třetích stran. V případě aktiv v oblasti IKT nebo součástí aktiv v oblasti IKT připravených k použití (tj. standardních aktiv nebo součástí) pořízených a používaných při provozu služeb IKT, které nepodporují zásadní nebo důležité funkce, finanční subjekty v co největší míře sledují používání knihoven třetích stran, včetně knihoven s otevřeným zdrojovým kódem.

Pro účely písmene f) finanční subjekty zohlední kritičnost zranitelnosti, klasifikaci stanovenou v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554 a rizikový profil aktiv v oblasti IKT, kterých se zjištěné zranitelnosti týkají.

3. V rámci politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou postupy řízení oprav.

4. Postupy řízení oprav uvedené v odstavci 3:

a) v rámci možností identifikují a vyhodnocují dostupné softwarové a hardwarové opravy a aktualizace pomocí automatizovaných nástrojů;

b) určují nouzové postupy pro opravu a aktualizaci aktiv v oblasti IKT;

c) testují a zavádějí softwarové a hardwarové opravy a aktualizace uvedené v čl. 8 odst. 2 písm. b) bodech v), vi) a vii);

d) stanoví lhůty pro instalaci oprav a aktualizací softwaru a hardwaru a postupy eskalace v případě, že tyto lhůty nelze dodržet.

Článek 11

Bezpečnost údajů a systémů

1. V rámci politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou postup pro zajištění bezpečnosti údajů a systémů.

2. Postup pro zajištění bezpečnosti údajů a systémů uvedený v odstavci 1 obsahuje všechny následující prvky týkající se bezpečnosti údajů a systémů IKT v souladu s klasifikací stanovenou podle čl. 8 odst. 1 nařízení (EU) 2022/2554:

a) omezení přístupu uvedená v článku 21 tohoto nařízení, která podporují požadavky na ochranu pro každý stupeň klasifikace;

b) určení základní úrovně bezpečné konfigurace aktiv v oblasti IKT, která minimalizuje riziko vystavení těchto aktiv v oblasti IKT kybernetickým hrozbám, a opatření k pravidelnému ověřování, zda jsou tyto základní úrovně konfigurace účinně zavedeny;

c) určení bezpečnostních opatření, která zajistí, že v systémech IKT a koncových zařízeních bude instalován pouze schválený software;

d) určení bezpečnostních opatření proti škodlivým kódům;

e) určení bezpečnostních opatření, která zajistí, aby se k přenosu a ukládání dat finančního subjektu používala pouze schválená média, systémy a koncová zařízení;

f) následující požadavky na zabezpečení používání přenosných koncových zařízení a soukromých nepřenosných koncových zařízení:

   i) požadavek na používání řešení pro vzdálenou správu koncových zařízení a vzdálené vymazání dat finančního subjektu;

   ii) požadavek na používání bezpečnostních mechanismů, které nemohou být neoprávněně upraveny, odstraněny nebo obejity zaměstnanci nebo poskytovateli služeb IKT z řad třetích stran;

   iii) požadavek na používání přenosných zařízení pro ukládání dat pouze v případě, že zbytkové riziko v oblasti IKT je v rozmezí přípustné odchylky rizika finančního subjektu uvedené v čl. 3 prvním pododstavci písm. a);

g) postup bezpečného vymazání dat, která se nacházejí v prostorách finančního subjektu nebo jsou uložena externě a která finanční subjekt již nepotřebuje shromažďovat nebo uchovávat;

h) postup bezpečné likvidace nebo vyřazení zařízení pro ukládání dat, která se nacházejí v prostorách finančního subjektu nebo jsou uložena externě a obsahují důvěrné informace;

i) určení a zavedení bezpečnostních opatření, která brání ztrátě a úniku dat ze systémů a koncových zařízení;

j) zavedení bezpečnostních opatření, která zajistí, že práce na dálku a používání soukromých koncových zařízení nebude mít nepříznivý dopad na bezpečnost IKT finančního subjektu;

k) v případě aktiv v oblasti IKT nebo služeb provozovaných poskytovateli služeb IKT z řad třetích stran určení a zavedení požadavků na zachování digitální provozní odolnosti v souladu s výsledky klasifikace dat a posouzení rizik v oblasti IKT.

Pro účely písmene b) zohledňuje základní úroveň bezpečné konfigurace uvedená v tomto písmenu osvědčené postupy a vhodné techniky stanovené v normách definovaných v čl. 2 bodě 1 nařízení (EU) č. 1025/2012.

Pro účely písmene k) zohlední finanční subjekty toto:

a) nastavení prvků provozovaných finančním subjektem v souladu s doporučeními dodavatele;

b) jasné rozdělení úloh a povinností v oblasti bezpečnosti informací mezi finanční subjekt a poskytovatele služeb IKT z řad třetích stran v souladu se zásadou plné odpovědnosti finančního subjektu za svého poskytovatele služeb IKT z řad třetích stran uvedenou v čl. 28 odst. 1 písm. a) nařízení (EU) 2022/2554 a v případě finančních subjektů uvedených v čl. 28 odst. 2 uvedeného nařízení v souladu s politikou finančního subjektu týkající se využívání služeb IKT podporujících zásadní nebo důležité funkce;

c) nutnost zajistit a udržovat v rámci finančního subjektu odpovídající kompetence v oblasti řízení a zajištění bezpečnosti při využívaní služby;

d) technická a organizační opatření k minimalizaci rizik spojených s infrastrukturou, kterou poskytovatel služeb IKT z řad třetích stran používá pro své služby IKT, a to s ohledem na osvědčené postupy a normy definované v čl. 2 bodě 1 nařízení (EU) č. 1025/2012.

Článek 12

Vedení protokolů

1. Finanční subjekty v rámci ochranných opatření proti vniknutí a zneužití údajů vypracují, zdokumentují a zavedou postupy, protokoly a nástroje pro vedení protokolů.

2. Postupy, protokoly a nástroje pro vedení protokolů uvedené v odstavci 1 obsahují všechny níže uvedené náležitosti:

a) identifikace událostí, které mají být protokolovány, doba uchovávání protokolů a opatření k zabezpečení a zpracování dat z protokolů s ohledem na účel, pro který jsou protokoly pořizovány;

b) sladění míry podrobnosti protokolů s jejich účelem a použitím, aby bylo možné účinně odhalovat neobvyklé aktivity, jak je uvedeno v článku 24;

c) požadavek na protokolování událostí, které souvisejí se všemi následujícími oblastmi:

   i) logické a fyzické řízení přístupu podle článku 21 a správa identit;

   ii) řízení kapacity;

   iii) řízení změn;

   iv) operace IKT, včetně činností systémů IKT;

   v) činnosti provozu sítí, včetně výkonnosti sítí IKT;

d) opatření na ochranu systémů vedení protokolů a informací z protokolů proti neoprávněné manipulaci, vymazání a neoprávněnému přístupu během uchovávání a přenosu a případně během používání;

e) opatření k detekci selhání systémů vedení protokolů;

f) aniž jsou dotčeny jakékoli platné regulační požadavky podle práva Unie nebo vnitrostátního práva, synchronizace hodin všech systémů IKT finančního subjektu s dokumentovaným spolehlivým referenčním zdrojem času.

Pro účely písmene a) stanoví finanční subjekty dobu uchovávání s přihlédnutím k obchodním cílům a cílům v oblasti bezpečnosti informací, důvodu pro zaznamenání události do protokolů a výsledkům posouzení rizik v oblasti IKT.

Oddíl 6

Bezpečnost sítí

Článek 13

Řízení bezpečnosti sítí

Finanční subjekty v rámci ochranných opatření zajišťujících bezpečnost sítí proti vniknutí a zneužití údajů vypracují, zdokumentují a zavedou politiky, postupy, protokoly a nástroje pro řízení bezpečnosti sítí, včetně všech následujících prvků:

a) oddělení a segmentace systémů a sítí IKT s ohledem na:

   i) zásadnost nebo důležitost funkce, kterou tyto systémy a sítě IKT podporují;

   ii) klasifikaci stanovenou v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554;

   iii) celkový rizikový profil aktiv v oblasti IKT využívajících tyto systémy a sítě IKT;

b) dokumentace všech síťových připojení a datových toků finančního subjektu;

c) používání oddělené a vyhrazené sítě pro správu aktiv v oblasti IKT;

d) stanovení a provádění kontrol přístupu k síti, aby se zabránilo tomu, že se k síti finančního subjektu připojí jakékoli neschválené zařízení nebo systém nebo jakýkoli koncový bod, který nesplňuje bezpečnostní požadavky finančního subjektu;

e) šifrování síťových spojení procházejících podnikovými sítěmi, veřejnými sítěmi, domácími sítěmi, sítěmi třetích stran a bezdrátovými sítěmi pro používané komunikační protokoly s přihlédnutím k výsledkům schválené klasifikace dat, výsledkům posouzení rizik v oblasti IKT a šifrování síťových spojení podle čl. 6 odst. 2;

f) koncepce sítí v souladu s požadavky na bezpečnost IKT stanovenými finančním subjektem s přihlédnutím k osvědčeným postupům pro zajištění důvěrnosti, integrity a dostupnosti sítě;

g) zabezpečení síťového provozu mezi interními sítěmi a internetem a dalšími externími připojeními;

h) stanovení úloh a povinností a kroků pro specifikaci, provádění, schvalování, změnu a revizi pravidel brány firewall a filtrů připojení;

i) přezkumy architektury sítě a návrhu zabezpečení sítě prováděné jednou za rok a pravidelně u mikropodniků, aby se zjistily potenciální zranitelnosti;

j) opatření pro případnou dočasnou izolaci dílčích sítí a síťových komponent a zařízení;

k) zavedení základní úrovně bezpečné konfigurace všech síťových komponent a zabezpečení („hardening“) sítě a síťových zařízení v souladu s pokyny dodavatele, případně s normami definovanými v čl. 2 bodě 1 nařízení (EU) č. 1025/2012 a s osvědčenými postupy;

l) postupy pro omezení, uzamčení a ukončení systémových a vzdálených relací po určité době nečinnosti;

m) v případě smluv o síťových službách:

   i) určení a specifikace opatření v oblasti bezpečnosti IKT a informací, úrovní služeb a požadavků na řízení všech síťových služeb;

   ii) to, zda tyto služby poskytuje poskytovatel služeb IKT v rámci skupiny nebo poskytovatelé služeb IKT z řad třetích stran.

Pro účely písmene h) provádějí finanční subjekty pravidelný přezkum pravidel brány firewall a filtrů připojení v souladu s klasifikací stanovenou podle čl. 8 odst. 1 nařízení (EU) 2022/2554 a s celkovým rizikovým profilem příslušných systémů IKT. U systémů IKT, které podporují zásadní nebo důležité funkce, musí finanční subjekty ověřovat přiměřenost stávajících pravidel brány firewall a filtrů připojení nejméně jednou za šest měsíců.

Článek 14

Zabezpečení informací během přenosu

1. V rámci ochranných opatření pro zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů finanční subjekty vypracují, zdokumentují a zavedou politiky, postupy, protokoly a nástroje na ochranu informací během přenosu. Finanční subjekty zajistí zejména všechny tyto prvky:

a) dostupnost, hodnověrnost, integrita a důvěrnost údajů během přenosu po síti a zavedení postupů pro hodnocení souladu s těmito požadavky;

b) prevence a detekce úniků dat a bezpečný přenos informací mezi finančním subjektem a externími stranami;

c) zavedení, zdokumentování a pravidelné přezkoumávání požadavků na opatření týkající se důvěrnosti nebo mlčenlivosti, které odrážejí potřeby finančního subjektu v oblasti ochrany informací a vztahují se na zaměstnance finančního subjektu, jakož i třetích stran.

2. Finanční subjekty navrhnou politiky, postupy, protokoly a nástroje na ochranu informací během přenosu uvedené v odstavci 1 na základě výsledků schválené klasifikace dat a posouzení rizik v oblasti IKT.

Oddíl 7

Řízení projektů a změn v oblasti IKT

Článek 15

Řízení projektů v oblasti IKT

1. V rámci ochranných opatření pro zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů finanční subjekty vypracují, zdokumentují a zavedou politiku pro řízení projektů v oblasti IKT.

2. Politika pro řízení projektů v oblasti IKT uvedená v odstavci 1 stanoví prvky, které zajišťují účinné řízení projektů v oblasti IKT souvisejících s pořízením, údržbou a případně rozvojem systémů IKT finančního subjektu.

3. Politika pro řízení projektů v oblasti IKT uvedená v odstavci 1 zahrnuje všechny tyto prvky:

a) cíle projektů v oblasti IKT;

b) správa a řízení projektů v oblasti IKT, včetně úloh a povinností;

c) plánování, časový rámec a kroky činěné v rámci projektů v oblasti IKT;

d) posouzení rizik projektů v oblasti IKT;

e) příslušné milníky;

f) požadavky na řízení změn;

g) testování všech požadavků, včetně bezpečnostních požadavků, a příslušný schvalovací proces pro spuštění systému IKT v produkčním prostředí.

4. Politika pro řízení projektů v oblasti IKT uvedená v odstavci 1 zajišťuje bezpečné provádění projektů v oblasti IKT tím, že poskytuje nezbytné informace a odborné znalosti z obchodní oblasti nebo funkcí, na které má projekt v oblasti IKT dopad.

5. V souladu s posouzením rizik projektů v oblasti IKT uvedeným v odst. 3 písm. d) stanoví politika pro řízení projektů v oblasti IKT uvedená v odstavci 1, že zahájení a průběh projektů v oblasti IKT, které mají dopad na zásadní nebo důležité funkce finančního subjektu, a s nimi spojená rizika jsou oznamovány vedoucímu orgánu takto:

a) jednotlivě nebo souhrnně, v závislosti na významu a velikosti projektů v oblasti IKT;

b) pravidelně a v případě potřeby na základě událostí.

Článek 16

Pořizování, vývoj a údržba systémů IKT

1. V rámci ochranných opatření pro zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů finanční subjekty vypracují, zdokumentují a zavedou politiku upravující pořizování, vývoj a údržbu systémů IKT. Tato politika:

a) identifikuje bezpečnostní postupy a metodiky týkající se pořizování, vývoje a údržby systémů IKT;

b) vyžaduje určení:

   i) technických specifikací a technických specifikací IKT vymezených v čl. 2 bodech 4 a 5 nařízení (EU) č. 1025/2012;

   ii) požadavků týkajících se pořizování, vývoje a údržby systémů IKT se zvláštním zaměřením na požadavky na bezpečnost IKT a na jejich schválení příslušnou obchodní funkcí a vlastníkem aktiv v oblasti IKT v souladu s interními pravidly správy a řízení finančního subjektu;

c) specifikuje opatření ke zmírnění rizika neúmyslné změny nebo úmyslné manipulace se systémy IKT během vývoje, údržby a spuštění těchto systémů IKT v produkčním prostředí.

2. Finanční subjekty vypracují, zdokumentují a zavedou postup pořizování, vývoje a údržby systémů IKT pro účely testování a schvalování všech systémů IKT před jejich použitím a po jejich údržbě v souladu s čl. 8 odst. 2 písm. b) body v), vi) a vii). Úroveň testování musí být úměrná významu příslušných obchodních postupů a aktiv v oblasti IKT. Testování musí být navrženo tak, aby ověřilo, že nové systémy IKT jsou vhodné k tomu, aby fungovaly tak, jak je zamýšleno, a že je zajištěna kvalita interně vyvinutého softwaru.

Ústřední protistrany nad rámec požadavků stanovených v prvním pododstavci podle potřeby zapojí do přípravy a provádění testování uvedeného v prvním pododstavci:

a) členy clearingového systému a klienty;

b) interoperabilní ústřední protistrany;

c) ostatní zúčastněné strany.

Centrální depozitáře cenných papírů nad rámec požadavků stanovených v prvním pododstavci podle potřeby zapojí do přípravy a provádění testování uvedeného v prvním pododstavci:

a) uživatele;

b) poskytovatele kritické technické infrastruktury a kritických služeb;

c) jiné centrální depozitáře cenných papírů;

d) jiné tržní infrastruktury;

e) všechny ostatní instituce, s nimiž centrální depozitáře cenných papírů ve své politice zachování provozu identifikovaly vzájemné závislosti.

3. Postup uvedený v odstavci 2 musí obsahovat provádění revizí zdrojového kódu, jež zahrnují statické i dynamické testování. Toto testování musí zahrnovat bezpečnostní testy systémů a aplikací, které jsou vystaveny vlivům internetu, v souladu s čl. 8 odst. 2 písm. b) body v), vi) a vii). Finanční subjekty:

a) identifikují a analyzují zranitelnosti a anomálie ve zdrojovém kódu;

b) přijmou akční plán k řešení těchto zranitelností a anomálií;

c) sledují provádění tohoto akčního plánu.

4. Postup uvedený v odstavci 2 zahrnuje bezpečnostní testování softwarových balíčků nejpozději ve fázi integrace v souladu s čl. 8 odst. 2 písm. b) body v), vi) a vii).

5. Postup uvedený v odstavci 2 stanoví, že:

a) v neprodukčních prostředích jsou uchovávána pouze anonymizovaná, pseudonymizovaná nebo náhodně vybraná produkční data;

b) finanční subjekty mají chránit integritu a důvěrnost dat v neprodukčních prostředích.

6. Odchylně od odstavce 5 může postup uvedený v odstavci 2 stanovit, že produkční data se ukládají pouze pro konkrétní příležitosti testování, na omezenou dobu a po schválení příslušnou funkcí a že tyto příležitosti musí být nahlášeny funkci řízení rizik v oblasti IKT.

7. Postup uvedený v odstavci 2 musí zahrnovat zavedení kontrolních mechanismů na ochranu integrity zdrojového kódu systémů IKT, které byly vyvinuty interně nebo poskytovatelem služeb IKT z řad třetích stran a dodány finančnímu subjektu poskytovatelem služeb IKT z řad třetích stran.

8. Postup uvedený v odstavci 2 stanoví, že proprietární software, a pokud je to možné, zdrojový kód buď poskytovaný poskytovateli služeb IKT z řad třetích stran, nebo pocházející z projektů s otevřeným zdrojovým kódem, musí být před spuštěním v produkčním prostředí analyzován a testován v souladu s odstavcem 3.

9. Odstavce 1 až 8 tohoto článku se vztahují rovněž na systémy IKT vyvinuté nebo spravované uživateli mimo funkci IKT, a to s využitím přístupu založeného na posouzení rizik.

Článek 17

Řízení změn v oblasti IKT

1. V rámci ochranných opatření pro zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů finanční subjekty zahrnou do postupů řízení změn v oblasti IKT uvedených v čl. 9 odst. 4 písm. e) nařízení (EU) 2022/2554 v souvislosti se všemi změnami softwarových, hardwarových a firmwarových komponent, systémů nebo bezpečnostních parametrů všechny následující prvky:

a) ověření, zda byly splněny požadavky na bezpečnost IKT;

b) mechanismy zajišťující nezávislost funkcí, které schvalují změny, a funkcí, které jsou odpovědné za žádosti o tyto změny a jejich provádění;

c) jasný popis úloh a povinností, aby bylo zajištěno, že:

   i) změny jsou upřesněny a plánovány;

   ii) je navržen odpovídající přechod;

   iii) změny jsou kontrolovaně testovány a dokončovány;

   iv) je účinným způsobem zajištěna kvalita;

d) dokumentace a podrobné informování o změnách, včetně:

   i) účelu a oblasti působnosti změny;

   ii) lhůty pro provedení změny;

   iii) očekávaných výsledků;

e) určení záložních postupů a odpovědnosti, včetně postupů a odpovědnosti za zrušení změn nebo obnovu po neúspěšně provedených změnách;

f) postupy, protokoly a nástroje pro řízení nouzových změn, které poskytují odpovídající záruky;

g) postupy pro dokumentování, přehodnocování, posuzování a schvalování nouzových změn po jejich zavedení, včetně náhradních řešení a oprav;

h) určení potenciálního dopadu změny na stávající bezpečnostní opatření v oblasti IKT a posouzení, zda taková změna vyžaduje přijetí dodatečných bezpečnostních opatření v oblasti IKT.

2. Ústřední protistrany a centrální depozitáře cenných papírů podrobí po provedení významných změn ve svých systémech IKT své systémy IKT přísnému testování pomocí simulace zátěžových podmínek.

Ústřední protistrany podle potřeby zapojí do přípravy a provádění testování uvedeného v prvním pododstavci:

a) členy clearingového systému a klienty;

b) interoperabilní ústřední protistrany;

c) ostatní zúčastněné strany.

Centrální depozitáře cenných papírů podle potřeby zapojí do přípravy a provádění testování uvedeného v prvním pododstavci:

a) uživatele;

b) poskytovatele kritické technické infrastruktury a kritických služeb;

c) jiné centrální depozitáře cenných papírů;

d) jiné tržní infrastruktury;

e) všechny ostatní instituce, s nimiž centrální depozitáře cenných papírů ve své politice zachování provozu IKT identifikovaly vzájemné závislosti.

Oddíl 8

Článek 18

Fyzická a environmentální bezpečnost

1. V rámci ochranných opatření pro zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů finanční subjekty stanoví, zdokumentují a zavedou politiku fyzické a environmentální bezpečnosti. Finanční subjekty vypracují tuto politiku s ohledem na prostředí kybernetických hrozeb, v souladu s klasifikací stanovenou podle čl. 8 odst. 1 nařízení (EU) 2022/2554 a s ohledem na celkový rizikový profil aktiv v oblasti IKT a přístupných informačních aktiv.

2. Politika fyzické a environmentální bezpečnosti uvedená v odstavci 1 zahrnuje všechny tyto prvky:

a) odkaz na oddíl politiky týkající se kontroly správy přístupových práv podle čl. 21 prvního pododstavce písm. g);

b) opatření na ochranu prostor, datových center finančního subjektu a určených citlivých oblastí vymezených finančním subjektem, v nichž se nacházejí aktiva v oblasti IKT a informační aktiva, před útoky, nehodami a environmentálními hrozbami a nebezpečími;

c) opatření k zabezpečení aktiv v oblasti IKT, a to jak v prostorách finančního subjektu, tak mimo ně, s přihlédnutím k výsledkům posouzení rizik v oblasti IKT týkajících se příslušných aktiv v oblasti IKT;

d) opatření k zajištění dostupnosti, hodnověrnosti, integrity a důvěrnosti aktiv v oblasti IKT, informačních aktiv a zařízení pro kontrolu fyzického přístupu finančního subjektu prostřednictvím odpovídající údržby;

e) opatření k zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů, včetně:

   i) politiky „čistého stolu“ pro tištěné dokumenty;

   ii) politiky „prázdné obrazovky“ u zařízení na zpracování informací.

Pro účely písmene b) musí být opatření na ochranu před environmentálními hrozbami a nebezpečími úměrná významu prostor, datových center a určených citlivých oblastí a významu operací nebo systémů IKT, které se v nich nacházejí.

Pro účely písmene c) musí politika fyzické a environmentální bezpečnosti uvedená v odstavci 1 zahrnovat opatření k zajištění vhodné ochrany aktiv v oblasti IKT, která jsou bez obsluhy.

KAPITOLA II

Politika v oblasti lidských zdrojů a řízení přístupu

Článek 19

Politika v oblasti lidských zdrojů

Finanční subjekty zahrnou do své politiky v oblasti lidských zdrojů nebo jiných příslušných politik všechny následující prvky související s bezpečností IKT:

a) určení a přidělení konkrétních povinností v oblasti bezpečnosti IKT;

b) požadavky na zaměstnance finančního subjektu a poskytovatele služeb IKT z řad třetích stran, kteří používají aktiva v oblasti IKT finančního subjektu nebo k nim mají přístup:

i) aby byli informováni o bezpečnostních zásadách, postupech a protokolech finančního subjektu souvisejících s IKT a dodržovali je;

ii) aby znali kanály pro podávání zpráv, které finanční subjekt zavedl pro detekci neobvyklého chování, včetně případných kanálů pro podávání zpráv zřízených v souladu se směrnicí Evropského parlamentu a Rady (EU) 2019/1937 ([11]);

iii) v případě zaměstnanců, aby po ukončení pracovního poměru vrátili finančnímu subjektu veškerá aktiva v oblasti IKT a hmotná informační aktiva, která mají v držení a která patří finančnímu subjektu.

Článek 20

Správa identit

1. V rámci kontroly správy přístupových práv finanční subjekty vypracují, zdokumentují a zavedou politiky a postupy správy identit, které zajistí jedinečnou identifikaci a autentizaci fyzických osob a systémů přistupujících k informacím finančních subjektů, aby bylo možné přidělovat uživatelská přístupová práva v souladu s článkem 21.

2. Politiky a postupy správy identit uvedené v odstavci 1 zahrnují všechny tyto prvky:

a) aniž je dotčen čl. 21 první pododstavec písm. c), musí být každému zaměstnanci finančního subjektu nebo zaměstnanci poskytovatelů služeb IKT z řad třetích stran, kteří mají přístup k informačním aktivům a aktivům v oblasti IKT finančního subjektu, přidělena jedinečná identita odpovídající jedinečnému uživatelskému účtu;

b) proces správy životního cyklu identit a účtů, který řídí vytváření, změny, kontrolu a aktualizaci, dočasnou deaktivaci a rušení všech účtů.

Pro účely písmene a) vedou finanční subjekty záznamy o všech přidělených identitách. Tyto záznamy se uchovávají i po reorganizaci finančního subjektu nebo po ukončení smluvního vztahu, aniž jsou dotčeny požadavky na uchovávání stanovené v použitelném právu Unie a vnitrostátním právu.

Pro účely písmene b) finanční subjekty zavedou, je-li to proveditelné a vhodné, pro proces správy identit v průběhu celého životního cyklu automatizovaná řešení.

Článek 21

Řízení přístupu

V rámci kontroly správy přístupových práv finanční subjekty vypracují, zdokumentují a zavedou politiku, která zahrnuje všechny následující prvky:

a) přidělování přístupových práv k aktivům v oblasti IKT na základě zásad „potřeba znát“ a „potřeba používat“ a zásady minimálních práv, a to i u vzdáleného a nouzového přístupu;

b) oddělení úkolů s cílem zabránit neoprávněnému přístupu ke kritickým údajům nebo zabránit přidělování kombinací přístupových práv, které lze využít k obcházení kontrol;

c) ustanovení o odpovědnosti uživatelů v tom smyslu, že se co nejvíce omezí používání obecných a sdílených uživatelských účtů a zajistí se, aby uživatelé byli vždy při provádění činností v systémech IKT identifikovatelní;

([11]) Směrnice Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie (Úř. věst. L 305, 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) ustanovení o omezení přístupu k aktivům v oblasti IKT, které stanoví kontrolní mechanismy a nástroje k zabránění neoprávněnému přístupu;

e) postupy v oblasti správy účtů pro udělování, změnu nebo odebírání přístupových práv k uživatelským a obecným účtům, včetně obecných účtů správců, zahrnující všechny následující prvky:

i) přidělení úloh a povinností týkajících se udělování, přezkumu a odebírání přístupových práv;

ii) přidělování privilegovaného, nouzového a administrátorského přístupu podle potřeby nebo v režimu *ad hoc* u všech systémů IKT;

iii) odebrání přístupových práv bez zbytečného odkladu po ukončení pracovního poměru nebo v případě, že přístup již není nutný;

iv) aktualizace přístupových práv, pokud je nezbytné provést změny a jinak nejméně jednou ročně u všech systémů IKT, které nepodporují zásadní nebo důležité funkce, a nejméně jednou za šest měsíců u systémů IKT, které podporují zásadní nebo důležité funkce;

f) metody ověřování zahrnující všechny tyto prvky:

i) používání metod ověřování, které jsou úměrné klasifikaci stanovené v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554 a celkovému rizikovému profilu aktiv v oblasti IKT a zohledňují osvědčené postupy;

ii) používání metod silného ověření v souladu s osvědčenými postupy a technikami pro vzdálený přístup do sítě finančního subjektu, pro privilegovaný přístup, pro přístup k aktivům v oblasti IKT podporujícím zásadní nebo důležité funkce nebo k veřejně přístupným aktivům v oblasti IKT;

g) opatření pro řízení fyzického přístupu zahrnující:

i) identifikaci a protokolování fyzických osob, které jsou oprávněny k přístupu do prostor, datových center a určených citlivých oblastí vymezených finančním subjektem, kde se nacházejí aktiva v oblasti IKT a informační aktiva;

ii) udělování fyzických přístupových práv ke kritickým aktivům v oblasti IKT pouze oprávněným osobám v souladu se zásadou „potřeba znát“ a zásadou minimálních práv a v režimu *ad hoc*;

iii) monitorování fyzického přístupu do prostor, datových center a určených citlivých oblastí vymezených finančním subjektem, kde se nacházejí aktiva v oblasti IKT nebo informační aktiva nebo obojí;

iv) přezkum fyzických přístupových práv s cílem zajistit, aby byla nepotřebná přístupová práva neprodleně odebrána.

Pro účely písm. e) bodu i) stanoví finanční subjekty dobu uchovávání s přihlédnutím k obchodním cílům a cílům v oblasti bezpečnosti informací, důvodům pro zaznamenání události do protokolů a výsledkům posouzení rizik v oblasti IKT.

Pro účely písm. e) bodu ii) používají finanční subjekty pro provádění administrativních úkolů v systémech IKT pokud možno vyhrazené účty. Je-li to proveditelné a vhodné, zavedou finanční subjekty pro řízení privilegovaného přístupu automatizovaná řešení.

Pro účely písm. g) bodu i) musí být identifikace a protokolování úměrné významu prostor, datových center, určených citlivých oblastí a významu operací nebo systémů IKT, které se v nich nacházejí.

Pro účely písm. g) bodu iii) musí být monitorování úměrné klasifikaci stanovené v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554 a významu oblasti, do níž je poskytnut přístup.

KAPITOLA III

Detekce a reakce v případě incidentů souvisejících s ikt

Článek 22

Politika pro řízení incidentů souvisejících s IKT

V rámci mechanismů pro detekci neobvyklých aktivit, včetně problémů s fungováním sítě IKT a incidentů souvisejících s IKT, finanční subjekty vypracují, zdokumentují a zavedou politiku pro incidenty související s IKT, prostřednictvím které:

a) dokumentují proces řízení incidentů souvisejících s IKT uvedený v článku 17 nařízení (EU) 2022/2554;

b) vypracují seznam příslušných kontaktů na interní funkce a externí zúčastněné strany, které se přímo podílejí na zajištění bezpečnosti operací IKT, včetně:

   i) detekce a monitorování kybernetických hrozeb;

   ii) detekce neobvyklých aktivit;

   iii) řízení zranitelností;

c) vypracují, zavedou a používají technické, organizační a provozní mechanismy na podporu procesu řízení incidentů souvisejících s IKT, včetně mechanismů umožňujících včasnou detekci neobvyklých aktivit a chování v souladu s článkem 23 tohoto nařízení;

d) uchovávají veškeré důkazy týkající se incidentů souvisejících s IKT po dobu, která není delší, než je nezbytné pro účely, pro které jsou údaje shromažďovány, a která je úměrná významu zasažených obchodních funkcí, podpůrných procesů a aktiv v oblasti IKT a informačních aktiv, v souladu s článkem 15 nařízení Komise v přenesené pravomoci (EU) 2024/1772 ([12]) a je v souladu s použitelným požadavkem na uchovávání podle práva Unie;

e) vypracují a zavedou mechanismy pro analýzu významných nebo opakujících se incidentů souvisejících s IKT a vzorců, pokud jde o počet a výskyt incidentů souvisejících s IKT.

Pro účely písmene d) uchovávají finanční subjekty důkazy uvedené v tomto písmenu bezpečným způsobem.

Článek 23

Detekce neobvyklých aktivit a kritéria pro detekci a reakci v případě incidentů souvisejících s IKT

1. Finanční subjekty stanoví jasné úlohy a povinnosti v oblasti účinné detekce a reakce v případě incidentů souvisejících s IKT a neobvyklých aktivit.

2. Mechanismus včasné detekce neobvyklých aktivit, včetně problémů s fungováním sítě IKT a incidentů souvisejících s IKT, jak je uveden v čl. 10 odst. 1 nařízení (EU) 2022/2554, umožní finančním subjektům:

a) shromažďovat, sledovat a analyzovat všechny následující prvky:

   i) interní a externí faktory, včetně přinejmenším protokolů shromážděných v souladu s článkem 12 tohoto nařízení, informací z obchodních funkcí a funkcí v oblasti IKT a všech problémů nahlášených uživateli finančního subjektu;

   ii) potenciální interní a externí kybernetické hrozby s ohledem na scénáře běžně používané aktéry hrozeb a scénáře založené na činnosti v oblasti operativních informací o hrozbách;

([12]) Nařízení Komise v přenesené pravomoci (EU) 2024/1772 ze dne 13. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, v nichž jsou upřesněna kritéria klasifikace incidentů souvisejících s IKT a kybernetických hrozeb, stanoveny prahové hodnoty významnosti a upřesněny údaje v hlášeních závažných incidentů (Úř. věst. L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) oznámení o incidentu souvisejícím s IKT od poskytovatele služeb IKT z řad třetích stran finančního subjektu, který byl detekován v systémech a sítích IKT poskytovatele služeb IKT z řad třetích stran a který může mít dopad na finanční subjekt;

b) určit neobvyklé aktivity a chování a zavést nástroje, které zasílají výstrahy týkající se neobvyklých aktivit a chování, přinejmenším u aktiv v oblasti IKT a informačních aktiv podporujících zásadní nebo důležité funkce;

c) stanovit pořadí výstrah uvedených v písmenu b), aby bylo možné řešit detekované incidenty související s IKT ve lhůtě, kterou finanční subjekt stanovil k jejich řešení, a to v pracovní i mimopracovní době;

d) automatizovanými prostředky nebo manuálně zaznamenávat, analyzovat a vyhodnocovat veškeré relevantní informace o všech neobvyklých aktivitách a chování.

Pro účely písmene b) zahrnují nástroje uvedené v tomto písmenu i nástroje, které zasílají automatické výstrahy na základě předem stanovených pravidel pro identifikaci anomálií, které mají dopad na úplnost a integritu zdrojů údajů nebo sběru protokolů.

3. Finanční subjekty chrání veškeré záznamy o neobvyklých činnostech proti neoprávněné manipulaci a neoprávněnému přístupu během jejich uchovávání a přenosu a případně také během jejich používání.

4. Finanční subjekty zaznamenávají všechny relevantní informace o každé zjištěné neobvyklé aktivitě tak, aby bylo možné:

a) určit den a čas výskytu neobvyklé aktivity;

b) určit den a čas detekce neobvyklé aktivity;

c) určit typ neobvyklé aktivity.

5. Finanční subjekty zohlední pro účely spuštění procesů detekce a reakce v případě incidentů souvisejících s IKT uvedených v čl. 10 odst. 2 nařízení (EU) 2022/2554 všechna následující kritéria:

a) náznaky, že v systému nebo síti IKT může být prováděna škodlivá aktivita nebo že tento systém nebo síť IKT mohly být ohroženy;

b) zjištění ztrát údajů ve vztahu k dostupnosti, hodnověrnosti, integritě a důvěrnosti údajů;

c) zjištění nepříznivého dopadu na transakce a operace finančního subjektu;

d) nedostupnost systémů a sítě IKT.

6. Pro účely odstavce 5 finanční subjekty rovněž zváží význam zasažených služeb.

KAPITOLA IV

Řízení zachování provozu IKT

Článek 24

Součásti politiky zachování provozu IKT

1. Finanční subjekty zahrnou do své politiky zachování provozu IKT uvedené v čl. 11 odst. 1 nařízení (EU) 2022/2554 všechny následující prvky:

a) popis:

i) cílů politiky zachování provozu IKT, včetně vzájemného vztahu mezi zachováním provozu IKT a celkovým zachováním provozu, a to s ohledem na výsledky analýzy dopadu na činnost uvedené v čl. 11 odst. 5 nařízení (EU) 2022/2554;

ii) rozsahu opatření, plánů, postupů a mechanismů pro zajištění zachování provozu IKT, včetně omezení a výjimek;

iii) časového rámce, na který se mají opatření, plány, postupy a mechanismy pro zajištění zachování provozu IKT vztahovat;

iv) kritérií pro aktivaci a deaktivaci plánů zachování provozu IKT, plánů reakce a obnovy v oblasti IKT a plánů krizové komunikace;

b) ustanovení týkající se:

i) řízení a organizace provádění politiky zachování provozu IKT, včetně úloh, povinností a postupů eskalace, které zajistí, že budou k dispozici dostatečné zdroje;

ii) souladu mezi plány zachování provozu IKT a plány celkového zachování provozu s ohledem přinejmenším na všechny následující prvky:

1) možné scénáře selhání, včetně scénářů uvedených v čl. 26 odst. 2 tohoto nařízení,

2) cíle obnovy, které stanoví, že finanční subjekt musí být po narušení schopen obnovit provoz svých zásadních nebo důležitých funkcí v rámci cílové doby a okamžiku obnovy;

iii) vypracování plánů zachování provozu IKT pro případy vážného narušení provozu a stanovení priorit opatření pro zachování provozu IKT s využitím přístupu založeného na posouzení rizik;

iv) vypracování, testování a přezkoumání plánů reakce a obnovy v oblasti IKT v souladu s články 25 a 26 tohoto nařízení;

v) přezkumu účinnosti zavedených opatření, plánů, postupů a mechanismů pro zachování provozu IKT v souladu s článkem 26 tohoto nařízení;

vi) uvedení politiky zachování provozu IKT do souladu s:

1) komunikační politikou podle čl. 14 odst. 2 nařízení (EU) 2022/2554,

2) opatřeními v oblasti komunikace a krizové komunikace uvedenými v čl. 11 odst. 2 písm. e) nařízení (EU) 2022/2554.

2. Kromě požadavků uvedených v odstavci 1 ústřední protistrany zajistí, aby jejich politika zachování provozu IKT:

a) obsahovala maximální dobu obnovy jejich zásadních funkcí, která není delší než dvě hodiny;

b) zohledňovala vnější vazby a vzájemné závislosti v rámci finančních infrastruktur, včetně obchodních systémů, jejichž clearing provádí ústřední protistrana, systémů vypořádání obchodů s cennými papíry a platebních systémů a úvěrových institucí využívaných ústřední protistranou nebo propojenou ústřední protistranou;

c) vyžadovala, aby byla zavedena opatření:

i) k zajištění zachování zásadních nebo důležitých funkcí ústřední protistrany na základě scénářů havárií;

ii) k udržování sekundárního místa zpracování, které je schopno zajistit zachování stejných zásadních nebo důležitých funkcí ústřední protistrany, jaké zajišťuje primární místo;

iii) k udržování sekundárního obchodního místa nebo zajištění okamžitého přístupu k němu, aby zaměstnanci mohli zajistit zachování služby v případě, že primární obchodní místo nebude k dispozici;

iv) ke zvážení, zda jsou zapotřebí další místa zpracování, zejména pokud různorodost rizikových profilů primárního a sekundárního místa neposkytuje dostatečnou jistotu, že cíle zachování provozu ústřední protistrany budou splněny ve všech scénářích.

Pro účely písmene a) dokončí ústřední protistrany postupy a platby ke konci dne v požadovaném čase a v požadovaný den za všech okolností.

Pro účely písmene c) bodu i) se opatření uvedená v tomto písmenu týkají dostupnosti odpovídajících lidských zdrojů, maximální doby výpadku zásadních funkcí a převzetí a obnovy na sekundárním místě.

Pro účely písmene c) bodu ii) musí mít sekundární místo zpracování uvedené v tomto písmenu profil rizika souvisejícího se zeměpisnou polohou odlišný od profilu primárního místa.

3. Kromě požadavků uvedených v odstavci 1 centrální depozitáře cenných papírů zajistí, aby jejich politika zachování provozu IKT:

a) zohledňovala veškeré vazby a vzájemné závislosti s uživateli, poskytovateli kritické technické infrastruktury a kritických služeb, jinými centrálními depozitáři cenných papírů a dalšími tržními infrastrukturami;

b) vyžadovala, aby její opatření pro zachování provozu IKT zajistila, že cílová doba obnovy jejich zásadních nebo důležitých funkcí nebude delší než dvě hodiny.

4. Kromě požadavků uvedených v odstavci 1 obchodní systémy zajistí, aby jejich politika zachování provozu IKT zajišťovala, že:

a) obchodování může být obnoveno přibližně do dvou hodin od rušivého incidentu;

b) maximální množství údajů, které může být ztraceno z jakékoli IT služby obchodního systému po rušivém incidentu, se blíží nule.

Článek 25

Testování plánů zachování provozu IKT

1. Při testování plánů zachování provozu IKT v souladu s čl. 11 odst. 6 nařízení (EU) 2022/2554 finanční subjekty zohlední analýzu dopadu na činnost finančního subjektu a posouzení rizik v oblasti IKT uvedené v čl. 3 odst. 1 písm. b) tohoto nařízení.

2. Finanční subjekty prostřednictvím testování svých plánů zachování provozu IKT uvedeného v odstavci 1 posoudí, zda jsou schopny zajistit zachování svých zásadních nebo důležitých funkcí. Toto testování:

a) je prováděno na základě testovacích scénářů, které simulují potenciální narušení, včetně odpovídajícího souboru závažných, ale pravděpodobných scénářů;

b) v příslušných případech zahrnuje testování služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran;

c) v případě finančních subjektů jiných než mikropodniky, jak je uvedeno v čl. 11 odst. 6 druhém pododstavci nařízení (EU) 2022/2554, zahrnuje scénáře přechodu z primární infrastruktury IKT na rezervní kapacitu, záložní a rezervní zařízení;

d) je navrženo tak, aby zpochybňovalo předpoklady, na nichž jsou založeny plány zachování provozu, včetně systému správy a řízení a plánů krizové komunikace;

e) obsahuje postupy pro ověření schopnosti zaměstnanců finančních subjektů, poskytovatelů služeb IKT z řad třetích stran, systémů IKT a služeb IKT adekvátně reagovat na scénáře, jež jsou řádně zohledněny v souladu s čl. 26 odst. 2.

Pro účely písmene a) musí finanční subjekty do testování vždy zahrnout scénáře zvažované pro vypracování plánů zachování provozu.

Pro účely písmene b) finanční subjekty důkladně zváží scénáře spojené s platební neschopností nebo selháním poskytovatelů služeb IKT z řad třetích stran nebo případně s politickými riziky v jurisdikcích poskytovatelů služeb IKT z řad třetích stran.

Pro účely písmene c) se testováním ověří, zda lze po dostatečně dlouhou dobu řádně vykonávat alespoň zásadní nebo důležité funkce a zda lze obnovit jejich běžný režim.

3. Nad rámec požadavků uvedených v odstavci 2 zapojí ústřední protistrany do testování svých plánů zachování provozu IKT uvedeného v odstavci 1:

a) členy clearingového systému;

b) externí poskytovatele;

c) příslušné instituce ve finanční infrastruktuře, s nimiž ústřední protistrany ve svých politikách zachování provozu identifikovaly vzájemné závislosti.

4. Kromě požadavků uvedených v odstavci 2 centrální depozitáře cenných papírů zapojí do testování svých plánů zachování provozu IKT uvedeného v odstavci 1 ve vhodných případech:

a) uživatele centrálních depozitářů cenných papírů;

b) poskytovatele kritické technické infrastruktury a kritických služeb;

c) jiné centrální depozitáře cenných papírů;

d) jiné tržní infrastruktury;

e) všechny ostatní instituce, s nimiž centrální depozitáře cenných papírů ve své politice zachování provozu identifikovaly vzájemné závislosti.

5. Výsledky testování uvedeného v odstavci 1 finanční subjekty zdokumentují. Veškeré zjištěné nedostatky vyplývající z tohoto testování se analyzují, řeší a oznamují vedoucímu orgánu.

Článek 26

Plány reakce a obnovy v oblasti IKT

1. Při vypracovávání plánů reakce a obnovy v oblasti IKT uvedených v čl. 11 odst. 3 nařízení (EU) 2022/2554 finanční subjekty zohlední výsledky analýzy dopadu na činnost finančního subjektu. Tyto plány reakce a obnovy v oblasti IKT:

a) specifikují podmínky, které vedou k jejich aktivaci nebo deaktivaci, a případné výjimky z této aktivace nebo deaktivace;

b) popisují, jaká opatření mají být přijata k zajištění dostupnosti, integrity, kontinuity a obnovy alespoň u systémů a služeb IKT, které podporují zásadní nebo důležité funkce finančního subjektu;

c) jsou navrženy tak, aby splňovaly cíle pro obnovu operací finančních subjektů;

d) jsou zdokumentovány a zpřístupněny zaměstnancům zapojeným do provádění plánů reakce a obnovy v oblasti IKT a jsou v případě nouze snadno dostupné;

e) poskytují krátkodobé i dlouhodobé možnosti obnovy, včetně částečné obnovy systémů;

f) stanoví cíle plánů reakce a obnovy v oblasti IKT a podmínky pro to, aby mohlo být konstatováno úspěšné provedení těchto plánů.

Pro účely písmene d) finanční subjekty jasně určí úlohy a povinnosti.

2. V plánech reakce a obnovy v oblasti IKT uvedených v odstavci 1 se určí příslušné scénáře, včetně scénářů závažných narušení činnosti a zvýšené pravděpodobnosti výskytu narušení. V těchto plánech jsou vypracovány scénáře založené na aktuálních informacích o hrozbách a na zkušenostech z předchozích případů narušení činnosti. Finanční subjekty řádně zohlední všechny následující scénáře:

a) kybernetické útoky a přechod z primární infrastruktury IKT na rezervní kapacitu, záložní a rezervní zařízení;

b) scénáře, při nichž se kvalita poskytování zásadní nebo důležité funkce sníží na nepřijatelnou úroveň nebo selže úplně, a potenciální dopad platební neschopnosti nebo jiných selhání jakéhokoli příslušného poskytovatele služeb IKT z řad třetích stran;

c) částečné nebo úplné selhání prostor, včetně kancelářských a obchodních prostor a datových center;

d) závažné selhání aktiv v oblasti IKT nebo komunikační infrastruktury;

e) nedostupnost kritického počtu zaměstnanců nebo zaměstnanců odpovědných za zajištění zachování provozu;

f) dopad změny klimatu a událostí souvisejících se zhoršováním životního prostředí, přírodních katastrof, pandemií a fyzických útoků, včetně vniknutí a teroristických útoků;

g) útoky zevnitř;

h) politická a sociální nestabilita, a to i případně v jurisdikci poskytovatele služeb IKT z řad třetích stran a v místě, kde jsou uloženy a zpracovávány údaje;

i) rozsáhlé výpadky proudu.

3. Pokud primární opatření pro obnovu nebudou v krátkodobém horizontu proveditelná z důvodu nákladů, rizik, logistiky nebo nepředvídaných okolností, zváží se v plánech reakce a obnovy v oblasti IKT uvedených v odstavci 1 alternativní možnosti.

4. V rámci plánů reakce a obnovy v oblasti IKT uvedených v odstavci 1 finanční subjekty zváží a zavedou opatření pro zajištění kontinuity s cílem zmírnit selhání poskytovatelů služeb IKT z řad třetích stran, kteří poskytují služby IKT podporující zásadní nebo důležité funkce finančního subjektu.

KAPITOLA V

Zpráva o přezkumu rámce pro řízení rizika v oblasti ikt

Článek 27

Formát a obsah zprávy o přezkumu rámce pro řízení rizika v oblasti IKT

1. Finanční subjekty předkládají zprávu o přezkumu rámce pro řízení rizika v oblasti IKT podle čl. 6 odst. 5 nařízení (EU) 2022/2554 v elektronickém formátu, který umožňuje vyhledávání.

2. Finanční subjekty uvedou ve zprávě podle odstavce 1 všechny následující informace:

a) úvodní část, která:

   i) jasně identifikuje finanční subjekt, jenž je předmětem zprávy, a v příslušných případech popisuje strukturu jeho skupiny;

   ii) popisuje kontext zprávy z hlediska povahy, rozsahu a složitosti služeb, činností a operací finančního subjektu, jeho organizace, určených zásadních funkcí, strategie, hlavních probíhajících projektů nebo činností, vztahů a jeho závislosti na interních a smluvních službách a systémech IKT nebo důsledků, které by měla úplná ztráta nebo závažné zhoršení těchto systémů z hlediska zásadních nebo důležitých funkcí a efektivity trhu;

   iii) shrnuje hlavní změny, k nimž došlo v rámci pro řízení rizika v oblasti IKT od předložení předchozí zprávy;

   iv) poskytuje shrnující přehled o současném a krátkodobém rizikovém profilu IKT, prostředí hrozeb, vyhodnocené účinnosti kontrolních mechanismů a o stavu zabezpečení finančního subjektu;

b) datum schválení zprávy vedoucím orgánem finančního subjektu;

c) popis důvodu přezkumu rámce pro řízení rizika v oblasti IKT v souladu s čl. 6 odst. 5 nařízení (EU) 2022/2554;

d) datum počátku a konce období přezkumu;

e) funkce, která je za přezkum odpovědná;

f) popis hlavních změn a zlepšení rámce pro řízení rizika v oblasti IKT, k nimž došlo od předchozího přezkumu;

g) shrnutí zjištění z přezkumu a podrobná analýza a posouzení závažnosti slabých míst, nedostatků a mezer v rámci pro řízení rizika v oblasti IKT zjištěných během období přezkumu;

h) popis opatření k odstranění zjištěných slabých míst, nedostatků a mezer, zahrnující všechny tyto prvky:

   i) souhrn opatření přijatých k nápravě zjištěných slabých míst, nedostatků a mezer;

   ii) předpokládaný termín provedení opatření a termíny související s vnitřní kontrolou provádění, včetně informací o stavu provádění těchto opatření ke dni vypracování zprávy s případným vysvětlením, zda existuje riziko, že termíny nebudou dodrženy;

   iii) nástroje, které mají být použity, a určení funkce, jež bude odpovědná za provádění opatření, a informace o tom, zda se jedná o interní nebo externí nástroje a funkce;

   iv) popis dopadu změn plánovaných v těchto opatřeních na rozpočtové, lidské a materiální zdroje finančního subjektu, včetně zdrojů určených na provádění nápravných opatření;

   v) v příslušných případech informace o postupu informování příslušného orgánu;

   vi) v případě, že se na zjištěná slabá místa, nedostatky nebo mezery nevztahují nápravná opatření, podrobné vysvětlení kritérií použitých k analýze dopadu těchto slabých míst, nedostatků nebo mezer za účelem vyhodnocení souvisejícího zbytkového rizika v oblasti IKT a kritérií použitých k přijetí souvisejícího zbytkového rizika;

i) informace o plánovaném dalším vývoji rámce pro řízení rizika v oblasti IKT;

j) závěry vyplývající z přezkumu rámce pro řízení rizika v oblasti IKT;

k) informace o předchozích přezkumech, včetně těchto informací:

   i) seznam předchozích přezkumů;

   ii) v relevantních případech stav provádění nápravných opatření stanovených v poslední zprávě;

   iii) v případě, že se nápravná opatření navržená v předchozích přezkumech ukázala jako neúčinná nebo způsobila neočekávané problémy, popis toho, jak by tato nápravná opatření mohla být zlepšena, nebo popis těchto neočekávaných problémů;

l) zdroje informací použité při vypracování zprávy, včetně všech následujících údajů:

   i) u finančních subjektů jiných než mikropodniky podle čl. 6 odst. 6 nařízení (EU) 2022/2554 výsledky interních auditů;

   ii) výsledky posouzení dodržování předpisů;

   iii) výsledky testování digitální provozní odolnosti a případně výsledky pokročilého testování nástrojů, systémů a procesů IKT na základě penetračního testování na základě hrozeb;

   iv) externí zdroje.

Pro účely písmene c), pokud byl přezkum zahájen na základě pokynů orgánů dohledu nebo závěrů vyvozených z příslušných procesů testování digitální provozní odolnosti nebo auditu, musí zpráva obsahovat výslovné odkazy na tyto pokyny nebo závěry, které umožní identifikovat důvod zahájení přezkumu. Pokud byl přezkum zahájen v návaznosti na incidenty související s IKT, obsahuje zpráva seznam všech incidentů souvisejících s IKT a analýzu hlavních příčin těchto incidentů.

Pro účely písmene f) musí popis obsahovat analýzu dopadu změn na strategii digitální provozní odolnosti finančního subjektu, na jeho interní kontrolní rámec v oblasti IKT a na jeho pravidla řízení rizika v oblasti IKT.

HLAVA III

ZJEDNODUŠENÝ RÁMEC PRO ŘÍZENÍ RIZIKA V OBLASTI IKT PRO FINANČNÍ SUBJEKTY UVEDENÉ V ČL. 16 ODST. 1 NAŘÍZENÍ (EU) 2022/2554

KAPITOLA I

Zjednodušený rámec pro řízení rizika v oblasti ikt

Článek 28

Řízení a organizace

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 musí mít zavedený interní řídicí a kontrolní rámec, který zajišťuje účinné a obezřetné řízení rizika v oblasti IKT s cílem dosáhnout vysoké úrovně digitální provozní odolnosti.

2. Finanční subjekty uvedené v odstavci 1 v rámci svého zjednodušeného rámce pro řízení rizika v oblasti IKT zajistí, aby jejich vedoucí orgán:

a) nesl celkovou odpovědnost za zajištění toho, aby zjednodušený rámec pro řízení rizika v oblasti IKT umožňoval dosažení obchodní strategie finančního subjektu v souladu s jeho ochotou podstupovat rizika, a zajistil, aby se riziko v oblasti IKT posuzovalo v tomto kontextu;

b) stanovil jasné úlohy a povinnosti pro všechny úkoly související s IKT;

c) stanovil cíle v oblasti bezpečnosti informací a požadavky na IKT;

d) schvaloval, kontroloval a pravidelně přezkoumával:

   i) klasifikaci informačních aktiv finančního subjektu podle čl. 30 odst. 1 tohoto nařízení, seznam hlavních zjištěných rizik a analýzu dopadu na činnost a související politiky;

   ii) plány zachování provozu finančního subjektu a opatření v oblasti reakce a obnovy uvedená v čl. 16 odst. 1 písm. f) nařízení (EU) 2022/2554;

e) přiděloval a alespoň jednou za rok přezkoumával rozpočtové prostředky potřebné k pokrytí potřeb finančního subjektu v oblasti digitální provozní odolnosti s ohledem na všechny typy zdrojů, včetně relevantních programů zvyšování povědomí o bezpečnosti v oblasti IKT a školení o digitální provozní odolnosti a zlepšování dovedností v oblasti IKT pro všechny zaměstnance;

f) specifikoval a zavedl politiky a opatření obsažené v kapitolách I, II a III této hlavy s cílem identifikovat, posuzovat a řídit riziko v oblasti IKT, kterému je finanční subjekt vystaven;

g) identifikoval a zavedl postupy, protokoly a nástroje IKT, které jsou nezbytné k ochraně všech informačních aktiv a aktiv v oblasti IKT;

h) zajistil, aby zaměstnanci finančního subjektu měli dostatečné znalosti a dovednosti k pochopení a posouzení rizika v oblasti IKT a jeho dopadu na operace finančního subjektu, a to přiměřeně k řízenému riziku v oblasti IKT;

i) stanovil způsoby podávání zpráv, včetně četnosti, formy a obsahu zpráv vedoucímu orgánu o bezpečnosti informací a digitální provozní odolnosti.

3. Finanční subjekty uvedené v odstavci 1 mohou v souladu s unijním a vnitrostátním odvětvovým právem svěřit úkoly v oblasti ověřování souladu s požadavky na řízení rizika v oblasti IKT poskytovatelům služeb IKT v rámci skupiny nebo poskytovatelům služeb IKT z řad třetích stran. V případě takového externího zadání nesou za ověřování souladu s požadavky na řízení rizika v oblasti IKT i nadále plnou odpovědnost finanční subjekty.

4. Finanční subjekty uvedené v odstavci 1 zajistí vhodné oddělení a nezávislost kontrolních funkcí a funkcí interního auditu.

5. Finanční subjekty uvedené v odstavci 1 zajistí, aby jejich zjednodušený rámec pro řízení rizika v oblasti IKT podléhal internímu auditu prováděnému auditory v souladu s plánem auditu finančních subjektů. Auditoři musí mít dostatečné znalosti, dovednosti a odborné znalosti, pokud jde o rizika v oblasti IKT, a musí být nezávislí. Četnost a zaměření auditů IKT musí být úměrné riziku finančního subjektu v oblasti IKT.

6. Na základě výsledku auditu uvedeného v odstavci 5 zajistí finanční subjekty uvedené v odstavci 1 včasné ověření a nápravu zásadních zjištění auditu IKT.

Článek 29

Politika a opatření v oblasti bezpečnosti informací

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 vypracují, zdokumentují a zavedou politiku bezpečnosti informací v kontextu zjednodušeného rámce pro řízení rizika v oblasti IKT. Tato politika bezpečnosti informací stanoví zásady a pravidla na vysoké úrovni pro zajištění ochrany důvěrnosti, integrity, dostupnosti a hodnověrnosti údajů a služeb, které tyto finanční subjekty poskytují.

2. Na základě své politiky bezpečnosti informací uvedené v odstavci 1 finanční subjekty uvedené v odstavci 1 zavedou a provádějí bezpečnostní opatření v oblasti IKT s cílem zmírnit své vystavení rizikům v oblasti IKT, včetně opatření ke zmírnění rizik prováděných poskytovateli služeb IKT z řad třetích stran.

Bezpečnostní opatření v oblasti IKT zahrnují všechna opatření uvedená v článcích 30 až 38.

Článek 30

Klasifikace informačních aktiv a aktiv v oblasti IKT

1. V rámci zjednodušeného rámce pro řízení rizika v oblasti IKT uvedeného v čl. 16 odst. 1 písm. a) nařízení (EU) 2022/2554 finanční subjekty uvedené v odstavci 1 uvedeného článku identifikují, klasifikují a zdokumentují všechny zásadní nebo důležité funkce, informační aktiva a aktiva v oblasti IKT, která je podporují, a jejich vzájemné závislosti. Finanční subjekty tuto identifikaci a klasifikaci podle potřeby přezkoumávají.

2. Finanční subjekty uvedené v odstavci 1 identifikují všechny zásadní nebo důležité funkce, které jsou podporovány poskytovateli služeb IKT z řad třetích stran.

Článek 31

Řízení rizika v oblasti IKT

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 zahrnou do svého zjednodušeného rámce pro řízení rizika v oblasti IKT všechny následující prvky:

a) stanovení přípustné odchylky rizika v oblasti IKT v souladu s ochotou finančního subjektu podstupovat riziko;

b) identifikace a posuzování rizik v oblasti IKT, kterým je finanční subjekt vystaven;

c) specifikace strategií zmírňování rizik alespoň pro rizika v oblasti IKT, která nejsou v rozmezí přípustné odchylky rizika finančního subjektu;

d) sledování účinnosti strategií zmírňování rizik uvedeného v písmenu c);

e) identifikace a posouzení všech rizik v oblasti bezpečnosti IKT a informací, která vyplývají z jakékoli významné změny systému nebo služeb IKT, procesů nebo postupů, z výsledků testování bezpečnosti IKT a po jakémkoli významném incidentu souvisejícím s IKT.

2. Finanční subjekty uvedené v odstavci 1 provádějí a dokumentují posuzování rizik v oblasti IKT pravidelně, úměrně jejich rizikovému profilu v oblasti IKT.

3. Finanční subjekty uvedené v odstavci 1 průběžně sledují hrozby a zranitelnosti, která se týkají jejich zásadních nebo důležitých funkcí a informačních aktiv a aktiv v oblasti IKT, a pravidelně přezkoumávají rizikové scénáře, které mají dopad na tyto zásadní nebo důležité funkce.

4. Finanční subjekty uvedené v odstavci 1 stanoví prahové hodnoty a kritéria výstrah pro spuštění a zahájení postupů reakce na incidenty související s IKT.

Článek 32

Fyzická a environmentální bezpečnost

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 určí a zavedou opatření fyzické bezpečnosti navržená na základě prostředí hrozeb a v souladu s klasifikací uvedenou v čl. 30 odst. 1 tohoto nařízení, s celkovým rizikovým profilem aktiv v oblasti IKT a přístupnými informačními aktivy.

2. Opatření uvedená v odstavci 1 chrání prostory finančních subjektů a případně datová centra finančních subjektů, v nichž se nacházejí aktiva v oblasti IKT a informační aktiva, před neoprávněným přístupem, útoky a nehodami a před environmentálními hrozbami a nebezpečími.

3. Ochrana před environmentálními hrozbami a nebezpečími musí být úměrná významu dotčených prostor a případně datových center a významu operací nebo systémů IKT, které se v nich nacházejí.

KAPITOLA II

Další prvky systémů, protokolů a nástrojů pro minimalizaci dopadu rizik v oblasti ikt

Článek 33

Řízení přístupu

Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 vypracují, zdokumentují a zavedou postupy pro řízení logického a fyzického přístupu a tyto postupy prosazují, sledují a pravidelně přezkoumávají. Tyto postupy zahrnují následující prvky řízení logického a fyzického přístupu:

a) přístupová práva k informačním aktivům, aktivům v oblasti IKT a jejich podporovaným funkcím a ke kritickým místům operací finančního subjektu jsou řízena na základě zásad „potřeba znát“ a „potřeba používat“ a zásady minimálních práv, a to i u vzdáleného a nouzového přístupu;

b) odpovědnost uživatelů, která zajišťuje, že uživatelé mohou být v souvislosti s činnostmi prováděnými v systémech IKT identifikováni;

c) postupy v oblasti správy účtů pro udělování, změnu nebo odebírání přístupových práv k uživatelským a obecným účtům, včetně obecných účtů správců:

d) metody ověřování, které jsou úměrné klasifikaci uvedené v čl. 30 odst. 1 a celkovému rizikovému profilu aktiv v oblasti IKT a které jsou založeny na osvědčených postupech;

e) přístupová práva jsou pravidelně přezkoumávána, a pokud již nejsou potřebná, jsou odebrána.

Pro účely písmene c) přiděluje finanční subjekt pro všechny systémy IKT privilegovaný, nouzový a administrátorský přístup podle potřeby nebo v režimu *ad hoc* a zaznamenává je v souladu s čl. 34 odst. 1 písm. f).

Pro účely písmene d) používají finanční subjekty metody silného ověření, které vycházejí z osvědčených postupů pro vzdálený přístup do sítě finančních subjektů, pro privilegovaný přístup a pro přístup k aktivům v oblasti IKT podporujícím zásadní nebo důležité funkce, které jsou veřejně přístupné.

Článek 34

Bezpečnost operací IKT

Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 v rámci svých systémů, protokolů a nástrojů a pro všechna aktiva v oblasti IKT:

a) sledují a řídí životní cyklus všech aktiv v oblasti IKT;

b) sledují, zda jsou aktiva v oblasti IKT případně podporována poskytovateli služeb IKT z řad třetích stran finančních subjektů;

c) určují požadavky na kapacitu svých aktiv v oblasti IKT a opatření k udržení a zlepšení dostupnosti a účinnosti systémů IKT a předcházení nedostatku kapacity IKT dříve, než se projeví;

d) provádějí automatické skenování a posuzování zranitelnosti aktiv v oblasti IKT úměrně jejich klasifikaci podle čl. 30 odst. 1 a celkovému rizikovému profilu aktiv v oblasti IKT a provádějí opravy za účelem odstranění zjištěných zranitelností;

e) řídí rizika spojená se zastaralými, nepodporovanými nebo původními aktivy v oblasti IKT;

f) protokolují události související s řízením logického a fyzického přístupu, s operacemi IKT, včetně činností v systému a v síti, a s řízením změn v oblasti IKT;

g) určují a zavádějí opatření pro monitorování a analýzu informací o neobvyklých aktivitách a chování u zásadních nebo důležitých operací IKT;

h) zavádějí opatření ke sledování relevantních a aktuálních informací o kybernetických hrozbách;

i) provádějí opatření k identifikaci možných úniků informací, škodlivých kódů a dalších bezpečnostních hrozeb a veřejně známých zranitelností softwaru a hardwaru a kontrolují, zda existují odpovídající nové bezpečnostní aktualizace.

Pro účely písmene f) musí finanční subjekty přizpůsobit míru podrobnosti protokolů jejich účelu a způsobu používání aktiva v oblasti IKT, které tyto protokoly vytváří.

Článek 35

Bezpečnost údajů, systémů a sítí

Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 v rámci svých systémů, protokolů a nástrojů vypracují a zavedou ochranná opatření, která zajistí bezpečnost sítí proti vniknutí a zneužití údajů a která zachovají dostupnost, hodnověrnost, integritu a důvěrnost údajů. S ohledem na klasifikaci uvedenou v čl. 30 odst. 1 tohoto nařízení zavedou finanční subjekty zejména všechny tyto prvky:

a) určení a zavedení opatření na ochranu údajů během jejich používání, přenosu i uchovávání;

b) určení a zavedení bezpečnostních opatření týkajících se používání softwaru, datových nosičů, systémů a koncových zařízení, které předávají a uchovávají data finančního subjektu;

c) určení a zavedení opatření k prevenci a odhalení neoprávněných připojení k síti finančního subjektu a k zabezpečení síťového provozu mezi interními sítěmi finančního subjektu a internetem a dalšími externími připojeními;

d) určení a zavedení opatření, která zajišťují dostupnost, hodnověrnost, integritu a důvěrnost údajů během síťových přenosů;

e) proces bezpečného vymazání údajů v prostorách nebo externě uchovávaných údajů, které již finanční subjekt nepotřebuje shromažďovat ani uchovávat;

f) proces bezpečné likvidace nebo vyřazení zařízení pro uchovávání údajů v prostorách nebo externě uložených zařízení pro uchovávání údajů, která obsahují důvěrné informace;

g) určení a zavedení opatření, která zajistí, že práce na dálku a používání soukromých koncových zařízení nebude mít nepříznivý dopad na schopnost finančního subjektu vykonávat své zásadní činnosti přiměřeným, včasným a bezpečným způsobem.

Článek 36

Testování bezpečnosti IKT

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 vypracují a zavedou plán testování bezpečnosti IKT za účelem ověření účinnosti svých bezpečnostních opatření v oblasti IKT vypracovaných v souladu s články 33, 34 a 35 a články 37 a 38 tohoto nařízení. Finanční subjekty zajistí, aby tento plán zohledňoval hrozby a zranitelnosti zjištěné v rámci zjednodušeného rámce pro řízení rizika v oblasti IKT uvedeného v článku 31 tohoto nařízení.

2. Finanční subjekty uvedené v odstavci 1 přezkoumají, posoudí a otestují bezpečnostní opatření v oblasti IKT s ohledem na celkový rizikový profil svých aktiv v oblasti IKT.

3. Finanční subjekty uvedené v odstavci 1 sledují a vyhodnocují výsledky bezpečnostních testů a u systémů IKT podporujících zásadní nebo důležité funkce bez zbytečného odkladu odpovídajícím způsobem aktualizují svá bezpečnostní opatření.

Článek 37

Pořizování, vývoj a údržba systémů IKT

Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 v příslušných případech navrhnou a zavedou postup, kterým se řídí pořizování, vývoj a údržba systémů IKT, přičemž uplatňují přístup založený na posouzení rizik. Tento postup:

a) zajistí, aby před jakýmkoli pořízením nebo vývojem systémů IKT byly jasně specifikovány funkční a jiné než funkční požadavky, včetně požadavků na bezpečnost informací, a aby je schválila příslušná obchodní funkce;

b) zajistí testování a schválení systémů IKT před jejich prvním použitím a před zavedením změn v produkčním prostředí;

c) určí opatření ke zmírnění rizika neúmyslné úpravy nebo úmyslné manipulace se systémy IKT během vývoje a zavádění v produkčním prostředí.

Článek 38

Řízení projektů a změn v oblasti IKT

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 vypracují, zdokumentují a zavedou postup řízení projektů v oblasti IKT a určí úlohy a odpovědnost za jeho provádění. Tento postup se vztahuje na všechny fáze projektů v oblasti IKT od jejich zahájení až po jejich ukončení.

2. Finanční subjekty uvedené v odstavci 1 vypracují, zdokumentují a zavedou postup řízení změn v oblasti IKT, aby zajistily, že všechny změny v systémech IKT budou zaznamenány, testovány, posouzeny, schváleny, provedeny a ověřeny řízeným způsobem a s odpovídajícími zárukami pro zachování digitální provozní odolnosti finančního subjektu.

KAPITOLA III

Řízení zachování provozu ikt

Článek 39

Součásti plánu zachování provozu IKT

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 vypracují své plány zachování provozu IKT s ohledem na výsledky analýzy jejich vystavení závažným narušením činnosti a možných dopadů těchto narušení a scénářů, kterým by mohla být vystavena jejich aktiva v oblasti IKT podporující zásadní nebo důležité funkce, včetně scénáře kybernetického útoku.

2. Plány zachování provozu IKT podle odstavce 1:

a) schvaluje vedoucí orgán finančního subjektu;

b) jsou zdokumentovány a snadno dostupné v případě naléhavé nebo krizové situace;

c) přidělují dostatečné zdroje na své provádění;

d) stanoví plánované úrovně obnovy a časové rámce pro obnovu a opětovné zahájení funkcí a klíčové interní a externí závislosti, včetně závislosti na poskytovatelích služeb IKT z řad třetích stran;

e) určují podmínky, za nichž může dojít k aktivaci plánů zachování provozu IKT, a jaká opatření mají být přijata k zajištění dostupnosti, kontinuity a obnovy aktiv finančních subjektů v oblasti IKT, která podporují zásadní nebo důležité funkce;

f) určují opatření pro obnovu zásadních nebo důležitých obchodních funkcí, podpůrných procesů, informačních aktiv a jejich vzájemné závislosti, aby se zabránilo nepříznivým dopadům na fungování finančních subjektů;

g) určují postupy a opatření pro zálohování, které specifikují rozsah údajů podléhajících zálohování a minimální frekvenci zálohování na základě významu funkce, která tyto údaje využívá;

h) zvažují alternativní možnosti v případech, kdy obnova nemusí být v krátkodobém horizontu proveditelná z důvodu nákladů, rizik, logistiky nebo nepředvídaných okolností;

i) specifikují interní a externí komunikační opatření, včetně plánů eskalace;

j) jsou aktualizovány v souladu se zkušenostmi získanými z incidentů, testů, zjištěných nových rizik a hrozeb, změněných cílů pro obnovu, významných změn v organizaci finančního subjektu a v aktivech v oblasti IKT podporujících zásadní nebo obchodní funkce.

Pro účely písmene f) opatření uvedená v tomto písmenu zajistí zmírnění selhání kritických poskytovatelů z řad třetích stran.

Článek 40

Testování plánů zachování provozu

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 testují své plány zachování provozu uvedené v článku 39 tohoto nařízení, včetně scénářů uvedených ve zmíněném článku, nejméně jednou ročně ohledně postupů zálohování a obnovy nebo při každé větší změně plánu zachování provozu.

2. Testování plánů zachování provozu uvedené v odstavci 1 musí prokázat, že finanční subjekty uvedené v témže odstavci jsou schopny udržet životaschopnost svých činností až do obnovení zásadních operací, a určí přitom případné nedostatky těchto plánů.

3. Finanční subjekty uvedené v odstavci 1 zdokumentují výsledky testování plánů zachování provozu, přičemž veškeré zjištěné nedostatky vyplývající z tohoto testování se analyzují, řeší a oznamují vedoucímu orgánu.

KAPITOLA IV

Zpráva o přezkumu zjednodušeného rámce pro řízení rizika v oblasti ikt

Článek 41

Formát a obsah zprávy o přezkumu zjednodušeného rámce pro řízení rizika v oblasti IKT

1. Finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554 předloží zprávu o přezkumu rámce pro řízení rizika v oblasti IKT uvedenou v odstavci 2 téhož článku v elektronickém formátu, který umožňuje vyhledávání.

2. Zpráva uvedená v odstavci 1 obsahuje všechny tyto informace:

a) úvodní část, která obsahuje:

   i) popis kontextu zprávy z hlediska povahy, rozsahu a složitosti služeb, činností a operací finančního subjektu, jeho organizace, určených zásadních funkcí, strategie, hlavních probíhajících projektů nebo činností, vztahů a závislosti finančního subjektu na interních a externích službách a systémech IKT nebo důsledků, které by měla úplná ztráta nebo závažné zhoršení těchto systémů na zásadní nebo důležité funkce a efektivitu trhu;

   ii) shrnující přehled o současném a krátkodobém identifikovaném riziku v oblasti IKT, prostředí hrozeb, vyhodnocené účinnosti kontrolních mechanismů a o stavu zabezpečení finančního subjektu;

   iii) informace o oznamované oblasti;

   iv) shrnutí hlavních změn rámce pro řízení rizika v oblasti IKT, k nimž došlo od předložení předchozí zprávy;

   v) shrnutí a popis dopadu hlavních změn zjednodušeného rámce pro řízení rizika v oblasti IKT, k nimž došlo od předložení předchozí zprávy;

b) v příslušných případech datum schválení zprávy vedoucím orgánem finančního subjektu;

c) popis důvodů přezkumu, včetně těchto informací:

   i) v případě, že byl přezkum zahájen na základě pokynů orgánů dohledu, doložení těchto pokynů;

   ii) v případě, že byl přezkum zahájen v důsledku výskytu incidentů souvisejících s IKT, seznam všech těchto incidentů souvisejících s IKT a související analýza hlavních příčin incidentů;

d) datum počátku a konce období přezkumu;

e) údaje o osobě odpovědné za přezkum;

f) shrnutí zjištění a vlastní hodnocení závažnosti zjištěných slabých míst, nedostatků a mezer v rámci pro řízení rizika v oblasti IKT během období přezkumu, včetně jejich podrobné analýzy;

g) stanovená opatření k nápravě zjištěných slabých míst, nedostatků a mezer ve zjednodušeném rámci pro řízení rizika v oblasti IKT a předpokládaný termín provedení těchto opatření, včetně následných opatření v souvislosti se slabými místy, nedostatky a mezerami zjištěnými v předchozích zprávách, pokud tato slabá místa, nedostatky a mezery dosud nebyly odstraněny;

h) celkové závěry přezkumu zjednodušeného rámce pro řízení rizika v oblasti IKT, včetně dalšího plánovaného vývoje.

HLAVA IV

ZÁVĚREČNÁ USTANOVENÍ

Článek 42

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. března 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN