EURÓPSKA
KOMISIA

V Bruseli 13. 3. 2024
C(2024) 1532 final

DELEGOVANÉ NARIADENIE KOMISIE (EÚ) …/…

z 13. 3. 2024,

ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa spresňujú nástroje, metódy, postupy a politiky riadenia IKT rizika a zjednodušený rámec riadenia IKT rizika

(Text s významom pre EHP)

DÔVODOVÁ SPRÁVA

1. KONTEXT DELEGOVANÉHO AKTU

Jedným z cieľov nariadenia (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA) je stanoviť jednotné požiadavky na bezpečnosť siete a informačných systémov spoločností a organizácií pôsobiacich vo finančnom sektore. Vytvára sa ním regulačný rámec pre digitálnu prevádzkovú odolnosť, v rámci ktorého musia všetky finančné subjekty zabezpečiť, aby dokázali odolávať všetkým typom narušení a hrozieb súvisiacich s IKT, reagovať na ne a zotaviť sa z nich. Tieto požiadavky sú rovnaké v celej EÚ, aby bolo možné predchádzať kybernetickým hrozbám a zmierňovať ich.

V tejto súvislosti podľa článku 15 prvého pododseku nariadenia DORA „*[e]urópske orgány dohľadu prostredníctvom spoločného výboru a po konzultácii s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) vypracujú spoločný návrh regulačných technických predpisov*“ s cieľom ďalej zabezpečiť „*harmonizáci[u] nástrojov, metód, postupov a politík riadenia IKT rizika*“ a podľa článku 16 vypracujú zjednodušený rámec riadenia IKT rizika pre určité finančné subjekty. Agentúra ENISA je podľa uvedeného súčasťou podvýboru Spoločného výboru európskych orgánov dohľadu pre digitálnu prevádzkovú odolnosť.

Toto delegované nariadenie zodpovedá uvedenému mandátu a bolo zaslané Komisii 17. januára 2024.

2. KONZULTÁCIE PRED PRIJATÍM AKTU

V rámci vypracúvania predpisov stanovených v tomto návrhu nariadenia európske orgány dohľadu 19. júna 2023 uverejnili návrh regulačných technických predpisov, pričom určili trojmesačné konzultačné obdobie, ktoré sa skončilo 11. septembra 2023. Európske orgány dohľadu dostali 120 odpovedí od rôznych účastníkov trhu z celého finančného sektora. Záverečná správa európskych orgánov dohľadu poskytuje úplný prehľad odpovedí zainteresovaných strán[1].

Respondenti verejnej konzultácie sa vyjadrili ku týmto aspektom navrhovaných regulačných technických predpisov:

- vyzvali na predĺženie lehoty na vykonávanie;
- vyzvali na dôraznejšiu proporcionalitu (napr. proporcionalitu, ktorá by sa uplatňovala oboma smermi, t. j. zohľadňovala by zvýšenú aj zníženú zložitosť a riziká; prístup špecifickejší pre daný sektor s osobitnou proporcionalitou napr. pre poisťovne...);
- vyzvali na vylúčenie riadiacich aspektov z návrhu regulačných technických predpisov, keďže sa zdá, že tieto sú mimo rozsahu mandátu, a
- vyzvali na to, aby sa neuvažovalo o dodatočných opatreniach pre zdroje cloud computingu.

[1] *Final report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554 [The European Supervisory Authorities (2024)]*, Záverečná správa o návrhu regulačných technických predpisov na ďalšiu harmonizáciu nástrojov, metód, postupov a politík riadenia IKT rizika, ako sa stanovuje v článku 15 a článku 16 ods. 3 nariadenia (EÚ) 2022/2554 [Európske orgány dohľadu (2024)].

Na základe prijatých pripomienok európske orgány dohľadu zaviedli do návrhu regulačných technických predpisov zmeny. Tieto zmeny sa týkali napr. zavedenia osobitnej proporcionality, odstránenia článku o riadení z požiadaviek na všeobecný režim, ako aj objasnenia určitých ustanovení, najmä tých, ktoré sú zahrnuté v článkoch týkajúcich sa aspektov bezpečnosti siete, šifrovania, kontroly prístupu a kontinuity činností. Európske orgány dohľadu sa vyjadrili proti zahrnutiu špecifických prvkov týkajúcich sa cloud computingu v záujme zachovania súladu so zásadou zabezpečenia technologickej neutrality. Európske orgány dohľadu sa namiesto toho rozhodli rozšíriť zvažované požiadavky tak, aby zahŕňali IKT aktíva alebo služby poskytované externými poskytovateľmi IKT služieb vo všeobecnosti. Pokiaľ však ide o lehoty na vykonávanie, európske orgány dohľadu neuvažovali o žiadnych zmenách, keďže tieto sú stanovené v nariadení DORA.

3. PRÁVNE PRVKY DELEGOVANÉHO AKTU

V hlave I kapitole I sa stanovuje hlavná zásada a prvky, ktoré treba zohľadniť pri vypracúvaní a vykonávaní politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT (článok 1).

V hlave II kapitole II sa stanovujú podmienky ďalšej harmonizácie nástrojov, metód, postupov a politík riadenia IKT rizika, pričom sa bližšie určujú: všeobecné prvky politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT (oddiel 1), osobitné prvky politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT (oddiel 2): úroveň tolerancie rizika, metodiky na vykonávanie posudzovania IKT rizika, opatrenia na riešenie IKT rizika, politika týkajúca sa riadenia IKT aktív (oddiel 3), politika týkajúca sa šifrovania a kryptografických kontrol (oddiel 4), politika týkajúca sa bezpečnosti operácií IKT (oddiel 5), politika riadenia týkajúca sa bezpečnosti siete (oddiel 6), politika riadenia IKT projektu (oddiel 7), politika fyzickej a environmentálnej bezpečnosti na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov (oddiel 8). V kapitole II sa stanovujú všetky bezpečnostné prvky IKT, ktoré finančné subjekty zahrnú do rozvoja svojich politík v oblasti ľudských zdrojov a kontroly prístupu. V kapitole III sa stanovujú všetky prvky politiky odhaľovania incidentov súvisiacich s IKT a reakcie na ne, ktoré finančné subjekty musia vypracovať a vykonávať. V kapitole IV sa stanovuje obsah a formát správy o preskúmaní rámca riadenia IKT rizika, ktorú sú finančné subjekty povinné vypracovať a predložiť.

V hlave III sa stanovuje zjednodušený rámec riadenia IKT rizika so zameraním na vytvorenie rámca správy a riadenia a kontroly (kapitola I), prístupový a kontrolný mechanizmus a požiadavky naň (kapitola II), vypracovanie plánu na zabezpečenie kontinuity činností v oblasti IKT (kapitola III), vypracovanie obsahu a formátu správy o preskúmaní rámca riadenia IKT rizika, ktorú sú finančné subjekty povinné vypracovať a predložiť (kapitola IV).

Hlava IV obsahuje záverečné ustanovenia o nadobudnutí účinnosti (článok 42).

DELEGOVANÉ NARIADENIE KOMISIE (EÚ) …/…

z 13. 3. 2024,

ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa spresňujú nástroje, metódy, postupy a politiky riadenia IKT rizika a zjednodušený rámec riadenia IKT rizika

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011[2], a najmä na jeho článok 15 štvrtý pododsek a článok 16 ods. 3 štvrtý pododsek,

keďže:

(1) Nariadenie (EÚ) 2022/2554 sa vzťahuje na širokú škálu finančných subjektov, ktoré sa líšia veľkosťou, štruktúrou, vnútornou organizáciou, povahou a zložitosťou činností, a teda majú zvýšené alebo znížené prvky zložitosti alebo rizík. S cieľom zabezpečiť riadne zohľadnenie uvedenej rozmanitosti by všetky požiadavky týkajúce sa politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT, ako aj zjednodušeného rámca riadenia IKT rizika, mali byť primerané veľkosti, štruktúre, vnútornej organizácii, povahe a zložitosti uvedených finančných subjektov a zodpovedajúcim rizikám.

(2) Z rovnakého dôvodu by finančné subjekty, na ktoré sa vzťahuje nariadenie (EÚ) 2022/2554, mali disponovať určitou flexibilitou, pokiaľ ide o spôsob, akým spĺňajú všetky požiadavky týkajúce sa politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT, ako aj zjednodušeného rámca riadenia IKT rizika. Preto by finančné subjekty mali mať možnosť používať každú dokumentáciu, ktorú už majú, na plnenie všetkých požiadaviek na dokumentáciu, ktoré vyplývajú z uvedených požiadaviek. Z toho vyplýva, že vypracovanie, dokumentácia a vykonávanie osobitných politík v oblasti bezpečnosti IKT by sa mali vyžadovať len v prípade určitých základných prvkov, pričom by sa okrem iného mali zohľadňovať najlepšie priemyselné postupy a normy. Okrem toho je na obsiahnutie osobitných technických aspektov vykonávania potrebné vypracovať, zdokumentovať a vykonávať postupy v oblasti bezpečnosti IKT tak, aby zahŕňali osobitné technické aspekty vykonávania vrátane riadenia kapacít a výkonnosti, riadenia zraniteľnosti a bezpečnostných záplat, bezpečnosti údajov a systému, ako aj vedenia záznamov.

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011(Ú. v. EÚ L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

(3) S cieľom zabezpečiť v priebehu času správne vykonávanie politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v hlave II kapitole I tohto nariadenia je dôležité, aby finančné subjekty správne prideľovali a zachovávali všetky úlohy a zodpovednosti týkajúce sa bezpečnosti IKT a aby sa v nich stanovili dôsledky nedodržiavania politík alebo postupov v oblasti bezpečnosti IKT.

(4) V záujme obmedzenia rizika konfliktu záujmov by finančné subjekty mali zabezpečiť, aby pri prideľovaní úloh a zodpovedností v oblasti IKT boli jednotlivé povinnosti oddelené.

(5) V snahe zabezpečiť flexibilitu a zjednodušiť kontrolný rámec finančných subjektov by sa od finančných subjektov nemalo vyžadovať, aby vypracúvali osobitné ustanovenia o dôsledkoch nedodržiavania politík, postupov a protokolov v oblasti bezpečnosti IKT uvedených v hlave II kapitole I tohto nariadenia, ak sú takéto ustanovenia už stanovené v inej politike alebo postupe.

(6) V dynamickom prostredí, v ktorom sa IKT riziká neustále vyvíjajú, je dôležité, aby finančné subjekty vypracovali svoj súbor politík v oblasti bezpečnosti IKT na základe popredných postupov a prípadne noriem vymedzených v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012[3]. To by malo umožniť finančným subjektom uvedeným v hlave II tohto nariadenia, aby boli neustále informované a pripravené reagovať na meniace sa prostredie.

(7) V záujme zabezpečenia svojej digitálnej prevádzkovej odolnosti by finančné subjekty uvedené v hlave II tohto nariadenia mali v rámci svojich politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT vypracovať a vykonávať politiku týkajúcu sa riadenia IKT aktív, postupy riadenia kapacít a výkonnosti, ako aj politiky a postupy pre operácie IKT. Uvedené politiky a postupy sú potrebné na zabezpečenie monitorovania stavu IKT aktív počas ich životného cyklu, aby sa tieto aktíva účinne používali a udržiavali (riadenie IKT aktív). Uvedené politiky a postupy by mali zabezpečiť aj optimalizáciu prevádzky IKT systémov, ako aj to, aby výkonnosť IKT systémov a kapacít spĺňala stanovené obchodné ciele a ciele informačnej bezpečnosti (riadenie kapacít a výkonnosti). Uvedené politiky a postupy by napokon mali zabezpečiť účinné a plynulé každodenné riadenie a prevádzku IKT systémov (operácie IKT), čím sa minimalizuje riziko straty dôvernosti, integrity a dostupnosti údajov. Uvedené politiky a postupy sú preto potrebné na zaistenie bezpečnosti sietí, stanovenie primeraných záruk proti vniknutiam a zneužitiu údajov a na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov.

(8) S cieľom zabezpečiť správne riadenie rizika pôvodných IKT systémov by finančné subjekty mali zaznamenávať a monitorovať dátumy ukončenia poskytovania podporných služieb zo strany externých poskytovateľov IKT služieb. Vzhľadom na možný vplyv, ktorý môže mať strata dôvernosti, integrity a dostupnosti údajov, by sa finančné subjekty mali pri zaznamenávaní a monitorovaní týchto dátumov ukončenia zameriavať na tie IKT aktíva alebo systémy, ktoré sú rozhodujúce pre obchodné operácie.

---

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho 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 ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(9) Kryptografickými kontrolami sa môže zabezpečiť dostupnosť, pravosť, integrita a dôvernosť údajov. Finančné subjekty uvedené v hlave II tohto nariadenia by preto mali identifikovať a vykonávať takéto kontroly na základe prístupu založeného na riziku. Na tento účel by finančné subjekty mali zašifrovať dotknuté údaje v pokoji, pri prenose alebo v prípade potreby pri používaní, a to na základe výsledkov dvojstupňového postupu, konkrétne klasifikácie údajov a komplexného posudzovania IKT rizika. Vzhľadom na zložitosť šifrovania údajov pri ich používaní by finančné subjekty uvedené v hlave II tohto nariadenia mali zašifrovať údaje pri používaní len vtedy, ak by to bolo vhodné vzhľadom na výsledky posudzovania IKT rizika. Ak však šifrovanie údajov pri ich používaní nie je uskutočniteľné alebo je príliš zložité, finančné subjekty uvedené v hlave II tohto nariadenia by mali mať možnosť ochraňovať dôvernosť, integritu a dostupnosť dotknutých údajov inými bezpečnostnými opatreniami v oblasti IKT. Vzhľadom na rýchly technologický vývoj v oblasti kryptografických techník by finančné subjekty uvedené v hlave II tohto nariadenia mali nepretržite držať krok s príslušným vývojom v oblasti kryptoanalýzy a zohľadňovať popredné postupy a normy. Finančné subjekty uvedené v hlave II tohto nariadenia by sa preto mali riadiť flexibilným prístupom založeným na zmierňovaní a monitorovaní rizika, aby dokázali riešiť dynamické prostredie kryptografických hrozieb vrátane hrozieb vyplývajúcich z kvantového pokroku.

(10) Na zabezpečenie dôvernosti, integrity a dostupnosti údajov sú nevyhnutné politiky, postupy, protokoly a nástroje týkajúce sa bezpečnosti operácií a prevádzky IKT. Jedným z kľúčových aspektov je prísne oddelenie produkčných prostredí IKT od prostredí, v ktorých sa IKT systémy vyvíjajú a testujú, alebo od iných neprodukčných prostredí. Toto oddelenie by malo slúžiť ako dôležité opatrenie v oblasti bezpečnosti IKT proti neúmyselnému a neoprávnenému prístupu k údajom, ich úpravám a vymazaniu v produkčnom prostredí, čo by mohlo viesť k závažným narušeniam obchodných operácií finančných subjektov uvedených v hlave II tohto nariadenia. Vzhľadom na súčasné postupy vývoja IKT systémov by však finančné subjekty za výnimočných okolností mali mať možnosť testovať v produkčných prostrediach za predpokladu, že takéto testovanie odôvodnia a získajú požadovaný súhlas.

(11) Rýchlo sa vyvíjajúci charakter IKT prostredí, zraniteľné miesta v oblasti IKT a kybernetické hrozby si vyžadujú proaktívny a komplexný prístup k identifikácii, vyhodnocovaniu a riešeniu zraniteľných miest v oblasti IKT. Bez takéhoto prístupu môžu byť finančné subjekty, ich zákazníci, používatelia alebo protistrany výrazne vystavené rizikám, ktoré by mohli ohroziť ich digitálnu prevádzkovú odolnosť, bezpečnosť ich sietí a dostupnosť, pravosť, integritu a dôvernosť údajov, ktoré by politiky a postupy v oblasti bezpečnosti IKT mali ochraňovať. Finančné subjekty uvedené v hlave II tohto nariadenia by preto mali identifikovať a odstraňovať zraniteľné miesta vo svojom IKT prostredí, pričom finančné subjekty aj ich externí poskytovatelia IKT služieb by mali dodržiavať koherentný, transparentný a zodpovedný rámec riadenia zraniteľnosti. Z rovnakého dôvodu by finančné subjekty mali monitorovať zraniteľné miesta v oblasti IKT tak, že budú využívať spoľahlivé zdroje a automatizované nástroje, prostredníctvom ktorých budú môcť overovať, či externí poskytovatelia IKT služieb urýchlene podnikajú v súvislosti so zraniteľnými miestami v poskytovaných IKT službách príslušné kroky.

(12) Kľúčovou súčasťou uvedených politík a postupov v oblasti bezpečnosti IKT, ktoré majú po otestovaní a nasadení v kontrolovanom prostredí odstrániť identifikované zraniteľné miesta a zabraňovať narušeniam pri inštalácii bezpečnostných záplat, by malo byť riadenie bezpečnostných záplat.

(13) Na zabezpečenie včasnej a transparentnej komunikácie o potenciálnych bezpečnostných hrozbách, ktoré by mohli mať vplyv na finančný subjekt a jeho zainteresované strany, by finančné subjekty mali stanoviť postupy zodpovedného informovania klientov, protistrán a verejnosti o zraniteľných miestach v oblasti IKT. Pri stanovovaní uvedených postupov by finančné subjekty mali zvažovať faktory vrátane závažnosti zraniteľnosti, potenciálneho vplyvu takejto zraniteľnosti na zainteresované strany a pripravenosti opravných alebo zmierňujúcich opatrení.

(14) S cieľom umožniť prideľovanie prístupových práv používateľom by finančné subjekty uvedené v hlave II tohto nariadenia mali zaviesť prísne opatrenia na zabezpečenie jedinečnej identifikácie jednotlivcov a systémov, ktorí/ktoré budú mať prístup k informáciám finančného subjektu. Ak by sa tak nestalo, finančné subjekty by boli vystavené potenciálnemu neoprávnenému prístupu, porušovaniu ochrany údajov a podvodným činnostiam, čím by sa ohrozila dôvernosť, integrita a dostupnosť citlivých finančných údajov. Zatiaľ čo používanie generických alebo spoločných účtov by malo byť výnimočne povolené za okolností, ktoré stanovia samotné finančné subjekty, finančné subjekty by mali zabezpečiť, aby ostala zachovaná zodpovednosť za opatrenia, ktoré sa prijmú prostredníctvom týchto účtov. Bez tejto záruky by potenciálni používatelia so zlými úmyslami mohli byť schopní brániť prijatiu vyšetrovacích a nápravných opatrení, v dôsledku čoho by finančné subjekty zostali zraniteľné voči neodhaleným nekalým činnostiam alebo sankciám ukladaným za nedodržiavanie predpisov.

(15) S cieľom riadiť rýchly pokrok v IKT prostrediach by finančné subjekty uvedené v hlave II tohto nariadenia mali zaviesť spoľahlivé politiky a postupy riadenia IKT projektu, aby sa zachovala dostupnosť, pravosť, integrita a dôvernosť údajov. V uvedených politikách a postupoch riadenia IKT projektu by sa mali identifikovať prvky, ktoré sú potrebné na úspešné riadenie IKT projektov, vrátane zmien, nadobudnutia, údržby a vývoja IKT systémov finančného subjektu, a to bez ohľadu na metodiku riadenia IKT projektu, ktorú si finančný subjekt zvolil. V kontexte uvedených politík a postupov by finančné subjekty mali prijať testovacie postupy a metódy, ktoré zodpovedajú ich potrebám, pričom by mali dodržiavať prístup založený na riziku a zabezpečiť zachovanie zabezpečeného, spoľahlivého a odolného IKT prostredia. S cieľom zaručiť bezpečné vykonávanie IKT projektu by finančné subjekty mali zabezpečiť, aby zamestnanci z konkrétnych podnikateľských oblastí alebo úloh, ktoré daný IKT projekt ovplyvňuje, mohli poskytovať potrebné informácie a odborné znalosti. V snahe zabezpečiť účinný dohľad by sa riadiacemu orgánu mali predkladať správy o IKT projektoch – a to najmä o projektoch, ktoré majú vplyv na kritické alebo dôležité funkcie, a o rizikách súvisiacich s nimi. Finančné subjekty by mali prispôsobovať frekvenciu a podrobnosti systematických a prebiehajúcich preskúmaní a správ významu a veľkosti dotknutých IKT projektov.

(16) Treba zabezpečiť, aby softvérové balíky, ktoré nadobudnú a vyvíjajú finančné subjekty uvedené v hlave II tohto nariadenia, boli účinne a bezpečne integrované do existujúceho IKT prostredia v súlade so stanovenými obchodnými cieľmi a cieľmi informačnej bezpečnosti. Finančné subjekty by preto mali takéto softvérové balíky dôkladne vyhodnocovať. Na tento účel a s cieľom identifikovať zraniteľné miesta a potenciálne nedostatky v oblasti bezpečnosti v rámci softvérových balíkov aj rozsiahlejších IKT systémov by finančné subjekty mali vykonávať testovanie bezpečnosti IKT. V snahe posúdiť integritu softvéru a zabezpečiť, aby používanie tohto softvéru neohrozovalo bezpečnosť IKT, by finančné subjekty mali preskúmať aj zdrojové kódy nadobudnutého softvéru vrátane, ak je to možné, proprietárneho

softvéru, ktorý poskytujú externí poskytovatelia IKT služieb, pričom sa použijú statické i dynamické metódy testovania.

(17) Bez ohľadu na rozsah zmien sa s týmito zmenami spájajú inherentné riziká, pričom tieto zmeny môžu predstavovať významné riziká v oblasti straty dôvernosti, integrity a dostupnosti údajov, čo by mohlo viesť k závažným narušeniam činnosti. Na ochranu finančných subjektov pred potenciálnymi zraniteľnými miestami a slabými miestami v oblasti IKT, ktoré by ich mohli vystaviť významným rizikám, je potrebný dôkladný proces overovania, aby sa potvrdilo, že všetky zmeny spĺňajú potrebné bezpečnostné požiadavky v oblasti IKT. Finančné subjekty uvedené v hlave II tohto nariadenia by preto ako základný prvok svojich politík a postupov v oblasti bezpečnosti IKT mali mať zavedené spoľahlivé politiky a postupy riadenia zmien IKT. V snahe zachovať objektivitu a účinnosť procesu riadenia zmien IKT, predchádzať konfliktom záujmov a zabezpečiť, aby sa zmeny IKT vyhodnocovali objektívne, treba oddeliť funkcie zodpovedné za schvaľovanie týchto zmien od funkcií, ktoré o vykonanie týchto zmien žiadajú a ktoré ich vykonávajú. Na dosiahnutie účinných prechodov, kontrolovaného vykonávania zmien IKT a minimálnych narušení prevádzky IKT systémov by finančné subjekty mali prideliť jasné úlohy a zodpovednosti, ktorými sa zabezpečí, aby sa zmeny IKT plánovali, primerane testovali a aby sa zabezpečila kvalita. S cieľom zabezpečiť, aby IKT systémy naďalej účinne fungovali, ako aj poskytovať záchrannú sieť pre finančné subjekty by finančné subjekty mali takisto vypracovať a zaviesť núdzové postupy. Finančné subjekty by mali jasne identifikovať tieto núdzové postupy a prideliť zodpovednosti tak, aby sa zabezpečila rýchla a účinná reakcia v prípade neúspešných zmien IKT.

(18) Na odhaľovanie, riadenie a nahlasovanie incidentov súvisiacich s IKT by finančné subjekty uvedené v hlave II tohto nariadenia mali zaviesť politiku incidentov súvisiacich s IKT, ktorá by zahŕňala zložky procesu riadenia incidentov súvisiacich s IKT. Na tento účel by finančné subjekty mali identifikovať všetky relevantné kontaktné osoby v rámci organizácie aj mimo nej, ktoré môžu uľahčiť správnu koordináciu a vykonávanie jednotlivých fáz tohto procesu. S cieľom optimalizovať odhaľovanie incidentov súvisiacich s IKT a reakciu na ne, ako aj identifikovať trendy v rámci týchto incidentov, ktoré sú cenným zdrojom informácií umožňujúcim finančným subjektom účinne identifikovať a riešiť základné príčiny a problémy, by finančné subjekty mali najmä podrobne analyzovať incidenty súvisiace s IKT, ktoré považujú za najvýznamnejšie, okrem iného z dôvodu ich pravidelného opätovného výskytu.

(19) V snahe zaručiť včasné a účinné odhalenie anomálnych činností by finančné subjekty uvedené v hlave II tohto nariadenia mali zhromažďovať, monitorovať a analyzovať rôzne zdroje informácií a mali by prideľovať príslušné úlohy a zodpovednosti. Pokiaľ ide o interné zdroje informácií, mimoriadne relevantným zdrojom sú záznamové protokoly, no finančné subjekty by sa nemali spoliehať výlučne na ne. Namiesto toho by finančné subjekty mali zohľadňovať širší rozsah informácií s cieľom zahrnúť údaje, ktoré ohlasujú iné interné funkcie, keďže uvedené funkcie sú často cenným zdrojom relevantných informácií. Z rovnakého dôvodu by finančné subjekty mali analyzovať a monitorovať informácie získané z externých zdrojov vrátane informácií poskytovaných externými poskytovateľmi IKT o incidentoch ovplyvňujúcich ich systémy a siete, ako aj iné zdroje informácií, ktoré finančné subjekty považujú za relevantné. Pokiaľ takéto informácie predstavujú osobné údaje, uplatňuje sa právo Únie v oblasti ochrany údajov. Osobné údaje by sa mali obmedziť na to, čo je nevyhnutné na odhaľovanie incidentov.

(20) Na uľahčenie odhaľovania incidentov súvisiacich s IKT by finančné subjekty mali uchovávať dôkazy o týchto incidentoch. S cieľom zabezpečiť na jednej strane, aby sa takéto dôkazy uchovávali dostatočne dlho, a aby sa na druhej strane zabránilo nadmernému regulačnému zaťaženiu, by finančné subjekty mali určiť lehotu na uchovávanie údajov okrem iného vzhľadom na kritickosť údajov a s ohľadom na požiadavky na uchovávanie údajov vyplývajúce z právnych predpisov Únie.

(21) Aby sa zabezpečilo včasné odhaľovanie incidentov súvisiacich s IKT, finančné subjekty uvedené v hlave II tohto nariadenia by nemali považovať kritériá určené na spustenie postupu odhaľovania incidentov súvisiacich s IKT a reakcie na ne za vyčerpávajúce. Zatiaľ čo finančné subjekty by mali zohľadniť každé z uvedených kritérií, nemalo by byť potrebné, aby sa okolnosti opísané v týchto kritériách vyskytovali súčasne, pričom ak sa majú spustiť procesy odhaľovania incidentov súvisiacich s IKT a reakcie na ne, primerane by sa mal zvážiť význam jednotlivých ovplyvnených IKT služieb.

(22) Pri vypracúvaní politiky kontinuity činností v oblasti IKT by finančné subjekty uvedené v hlave II tohto nariadenia mali zohľadňovať základné zložky riadenia IKT rizika vrátane riadenia incidentov súvisiacich s IKT a komunikačných stratégií, procesu riadenia zmien IKT a riziká spojené s externými poskytovateľmi IKT služieb.

(23) Treba vypracovať súbor scenárov, ktoré by finančné subjekty uvedené v hlave II tohto nariadenia mali zohľadňovať tak pri vykonávaní plánov reakcie a obnovy v oblasti IKT, ako aj pri testovaní plánov na zabezpečenie kontinuity činností v oblasti IKT. Uvedené scenáre by mali slúžiť ako východiskový bod pre finančné subjekty na analýzu relevantnosti a vierohodnosti každého scenára, ako aj potreby vypracovať alternatívne scenáre. Finančné subjekty by sa mali zamerať na tie scenáre, v rámci ktorých by investície do opatrení na zvýšenie odolnosti mohli byť efektívnejšie a účinnejšie. Testovaním prepnutia medzi primárnou infraštruktúrou IKT a akoukoľvek redundantnou kapacitou, zálohami a redundantnými zariadeniami by finančné inštitúcie mali posúdiť, či uvedená kapacita, zálohy a uvedené zariadenia fungujú účinne počas dostatočne dlhého obdobia, a zabezpečiť obnovenie normálneho fungovania primárnej infraštruktúry IKT v súlade s cieľmi obnovy.

(24) Treba stanoviť požiadavky na operačné riziko a konkrétnejšie požiadavky na riadenie IKT projektu a zmien, ako aj riadenie kontinuity činností v oblasti IKT na základe požiadaviek, ktoré sa už uplatňujú na centrálne protistrany podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012[4], centrálne depozitáre cenných papierov podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 600/2014[5] a obchodné miesta podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 909/2014[6].

---

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012 (Ú. v. EÚ L 173, 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

[6] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(25) V článku 6 ods. 5 nariadenia (EÚ) 2022/2554 sa vyžaduje, aby finančné subjekty preskúmali svoj rámec riadenia IKT rizika a predložili svojmu príslušnému orgánu správu o tomto preskúmaní. S cieľom umožniť príslušným orgánom uľahčené spracúvanie informácií v týchto správach a zaručiť primeraný prenos uvedených informácií by finančné subjekty mali tieto správy predkladať v elektronickom formáte s možnosťou vyhľadávania.

(26) Požiadavky na finančné subjekty, na ktoré sa vzťahuje zjednodušený rámec riadenia IKT rizika uvedený v článku 16 nariadenia (EÚ) 2022/2554, by sa mali zameriavať na tie kľúčové oblasti a prvky, ktoré sú vzhľadom na rozsah, riziko, veľkosť a zložitosť uvedených finančných subjektov minimálne potrebné na zabezpečenie dôvernosti, integrity, dostupnosti a pravosti údajov a služieb týchto finančných subjektov. V tejto súvislosti by tieto finančné subjekty mali mať zavedený rámec vnútornej správy, riadenia a kontroly s jasnými zodpovednosťami, aby sa mohol dosiahnuť účinný a spoľahlivý rámec riadenia rizík. S cieľom znížiť administratívne a prevádzkové zaťaženie by uvedené finančné subjekty mali navyše vypracovať a zdokumentovať len jednu politiku, t. j. politiku v oblasti informačnej bezpečnosti, v ktorej sa spresňujú zásady a pravidlá na vysokej úrovni potrebné na ochranu dôvernosti, integrity, dostupnosti a pravosti údajov a služieb týchto finančných subjektov.

(27) Ustanovenia tohto nariadenia sa týkajú oblasti rámca riadenia IKT rizika, pričom podrobne opisujú konkrétne prvky uplatniteľné na finančné subjekty v súlade s článkom 15 nariadenia (EÚ) 2022/2554 a navrhujú zjednodušený rámec riadenia IKT rizika pre finančné subjekty stanovený v článku 16 ods. 1 uvedeného nariadenia. V snahe zabezpečiť súdržnosť medzi bežným a zjednodušeným rámcom riadenia IKT rizika a keďže uvedené ustanovenia by sa mali začať uplatňovať súčasne, je vhodné zahrnúť tieto ustanovenia do jedného legislatívneho aktu.

(28) Toto nariadenie vychádza z návrhu regulačných technických predpisov, ktoré Komisii predložili Európsky orgán pre bankovníctvo, Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov a Európsky orgán pre cenné papiere a trhy (európske orgány dohľadu) po konzultácii s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA).

(29) Spoločný výbor európskych orgánov uvedený v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010[7], v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010[8] a v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010[9] uskutočnil otvorené verejné konzultácie k návrhu regulačných technických predpisov, z ktorých toto nariadenie vychádza, analyzoval potenciálne náklady a prínosy navrhovaných predpisov a požiadal o poradenstvo Skupinu zainteresovaných strán v bankovníctve zriadenú v súlade

---

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

[8] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

[9] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES (Ú. v. EÚ L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010, Skupinu zainteresovaných strán v poisťovníctve a zaisťovníctve a skupinu zainteresovaných strán v dôchodkovom poistení zamestnancov zriadené v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 a Skupinu zainteresovaných strán v oblasti cenných papierov a trhov zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010.

(30) V rozsahu, v akom sa na plnenie povinností stanovených v tomto akte vyžaduje spracúvanie osobných údajov, by sa malo v plnej miere uplatňovať nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 a nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018. Dodržiavať by sa napríklad mala zásada minimalizácie údajov, ak dochádza k zhromažďovaniu osobných údajov, aby sa zabezpečilo primerané odhaľovanie incidentov. Návrh znenia tohto aktu bol konzultovaný aj s európskym dozorným úradníkom pre ochranu údajov,

PRIJALA TOTO NARIADENIE:

HLAVA I
VŠEOBECNÉ ZÁSADY

Článok 1
Celkový rizikový profil a zložitosť

Pri vypracúvaní a vykonávaní politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v hlave II a zjednodušeného rámca riadenia IKT rizika uvedeného v hlave III sa zohľadňuje veľkosť a celkový rizikový profil finančného subjektu, ako aj povaha, rozsah a prvky zvýšenej alebo zníženej zložitosti jeho služieb, činností a operácií vrátane prvkov týkajúcich sa:

a) šifrovania a kryptografie;

b) bezpečnosti operácií IKT;

c) bezpečnosti siete;

d) riadenia IKT projektu a zmien;

e) potenciálneho vplyvu IKT rizika na dôvernosť, integritu a dostupnosť údajov, ako aj narušení na kontinuitu a dostupnosť činností finančného subjektu.

HLAVA II
ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, POSTUPOV A POLITÍK RIADENIA IKT RIZIKA V SÚLADE S ČLÁNKOM 15 NARIADENIA (EÚ) 2022/2554

KAPITOLA I
POLITIKY, POSTUPY, PROTOKOLY A NÁSTROJE V OBLASTI BEZPEČNOSTI IKT

ODDIEL 1

Článok 2

Všeobecné prvky politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT

1. Finančné subjekty zabezpečia, aby ich politiky v oblasti bezpečnosti IKT, informačná bezpečnosť a súvisiace postupy, protokoly a nástroje uvedené v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 boli začlenené do ich rámca riadenia IKT rizika. Finančné subjekty zavedú politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT stanovené v tejto kapitole, ktoré:

   a) zaistia bezpečnosť sietí;

   b) obsahujú ochranné opatrenia proti vniknutiam a zneužitiu údajov;

   c) zachovávajú dostupnosť, pravosť, integritu a dôvernosť údajov, a to aj prostredníctvom kryptografických techník;

   d) zaručia presný a urýchlený prenos údajov bez závažných narušení a zbytočných prieťahov.

2. Finančné subjekty zabezpečia, aby politiky v oblasti bezpečnosti IKT uvedené v odseku 1:

   a) boli zosúladené s cieľmi informačnej bezpečnosti finančného subjektu zahrnutými do stratégie digitálnej prevádzkovej odolnosti uvedenej v článku 6 ods. 8 nariadenia (EÚ) 2022/2554;

   b) obsahovali dátum, kedy riadiaci orgán formálne schválil politiky v oblasti bezpečnosti IKT;

   c) obsahovali ukazovatele a opatrenia s cieľom:

      i) monitorovať vykonávanie politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT;

      ii) zaznamenávať výnimky z tohto vykonávania;

      iii) zaistiť, aby bola zabezpečená digitálna prevádzková odolnosť finančného subjektu v prípade výnimiek uvedených v bode ii);

   d) stanovovali povinnosti zamestnancov na všetkých úrovniach, aby sa zaistila bezpečnosť IKT finančného subjektu;

e) bližšie určovali dôsledky nedodržiavania politík v oblasti bezpečnosti IKT zo strany zamestnancov finančného subjektu, ak ustanovenia na tento účel nie sú stanovené v iných politikách finančného subjektu;

f) obsahovali zoznam dokumentácie, ktorá sa má viesť;

g) bližšie určovali opatrenia na segregáciu povinností v kontexte modelu troch línií obrany alebo prípadne iného interného modelu riadenia a kontroly rizík s cieľom zabrániť konfliktom záujmov;

h) zohľadňovali popredné postupy a prípadne normy v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012;

i) identifikovali úlohy a zodpovednosti za vypracovanie, vykonávanie a udržiavanie politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT;

j) boli predmetom preskúmania v súlade s článkom 6 ods. 5 nariadenia (EÚ) 2022/2554;

k) zohľadňovali závažné zmeny týkajúce sa finančného subjektu vrátane závažných zmien činností alebo postupov finančného subjektu, panorámy kybernetických hrozieb alebo uplatniteľných právnych povinností.

ODDIEL 2

Článok 3
Riadenie IKT rizika

Finančné subjekty vypracujú, zdokumentujú a vykonávajú politiky a postupy riadenia IKT rizika, ktoré obsahujú všetky tieto prvky:

a) údaj o schválení úrovne tolerancie rizika v prípade IKT rizika stanoveného v súlade s článkom 6 ods. 8 písm. b) nariadenia (EÚ) 2022/2554;

b) postup a metodiku na vykonávanie posudzovania IKT rizika, v ktorých sa identifikujú:

   i) zraniteľné miesta a hrozby, ktoré ovplyvňujú alebo môžu ovplyvniť podporované obchodné funkcie, IKT systémy a IKT aktíva podporujúce uvedené funkcie;

   ii) kvantitatívne alebo kvalitatívne ukazovatele na meranie vplyvu a pravdepodobnosti zraniteľných miest a hrozieb uvedených v bode i);

c) postup identifikácie, vykonávania a dokumentácie opatrení na riešenie IKT rizika v prípade identifikovaných a posudzovaných IKT rizík vrátane určenia opatrení na riešenie IKT rizika, ktoré sú potrebné na to, aby sa IKT riziko dostalo do úrovne tolerancie rizika uvedenej v písmene a);

d) v prípade zvyškových IKT rizík, ktoré sú stále prítomné po vykonaní opatrení na riešenie IKT rizika uvedených v písmene c):

   i) ustanovenia o identifikácii uvedených zvyškových IKT rizík;

   ii) pridelenie úloh a zodpovedností, pokiaľ ide o:

      1. akceptovanie zvyškových IKT rizík, ktoré prekračujú úroveň tolerancie voči riziku finančného subjektu uvedenú v písmene a);

2. postup preskúmania uvedený v bode iv) tohto písmena d);

iii) vypracovanie zoznamu akceptovaných zvyškových IKT rizík vrátane uvedenia dôvodu, prečo boli akceptované;

iv) ustanovenia o preskúmaní akceptovaných zvyškových IKT rizík aspoň raz ročne vrátane:

1. identifikácie všetkých zmien zvyškových IKT rizík;

2. posúdenia dostupných zmierňujúcich opatrení;

3. posúdenia toho, či sú dôvody na akceptovanie zvyškových IKT rizík stále platné a uplatniteľné k dátumu preskúmania;

e) ustanovenia o monitorovaní:

i) všetkých zmien panorámy hrozieb IKT rizika a kybernetických hrozieb;

ii) vnútorných a vonkajších zraniteľných miest a hrozieb;

iii) IKT rizika finančného subjektu, ktoré umožňuje rýchle odhalenie zmien, ktoré by mohli ovplyvniť jeho profil IKT rizika;

f) ustanovenia o postupe na zabezpečenie toho, aby sa zohľadnili všetky zmeny obchodnej stratégie a stratégie digitálnej prevádzkovej odolnosti finančného subjektu.

Na účely prvého odseku písm. c) sa postupom uvedeným v uvedenom písmene zabezpečí:

a) monitorovanie účinnosti zavedených opatrení na riešenie IKT rizika;

b) posúdenie toho, či sa dosiahli stanovené úrovne tolerancie rizika finančného subjektu;

c) posúdenie toho, či finančný subjekt v prípade potreby prijal opatrenia na nápravu alebo zlepšenie týchto opatrení.

ODDIEL 3
RIADENIE IKT AKTÍV

Článok 4
Politika v oblasti riadenia IKT aktív

1. V rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú politiku riadenia IKT aktív.

2. Politikou riadenia IKT aktív uvedenou v odseku 1 sa:

a) stanoví monitorovanie a riadenie životného cyklu IKT aktív identifikovaných a klasifikovaných v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554;

b) stanoví, aby finančný subjekt viedol záznamy o všetkých týchto prvkoch:

i) jedinečný identifikátor každého IKT aktíva;

ii) informácie o umiestnení – či už fyzickom alebo logickom – všetkých IKT aktív;

iii) klasifikácia všetkých IKT aktív uvedená v článku 8 ods. 1 nariadenia (EÚ) 2022/2254;

iv) totožnosť vlastníkov IKT aktív;

v) obchodné funkcie alebo služby podporované IKT aktívom;

vi) požiadavky na kontinuitu činností v oblasti IKT vrátane časových cieľov obnovy a cieľov bodu obnovy;

vii) či IKT aktívum môže byť alebo je vystavené externým sieťam vrátane internetu;

viii) prepojenia a vzájomné závislosti medzi IKT aktívami a obchodnými funkciami využívajúcimi každé IKT aktívum;

ix) v náležitých prípadoch v prípade všetkých IKT aktív dátumy ukončenia pravidelných, rozšírených a špecifických podporných služieb externého poskytovateľa IKT služieb, po ktorých ukončení už tieto IKT aktíva nie sú podporované ich dodávateľom alebo externým poskytovateľom IKT služieb;

c) stanoví v prípade finančných subjektov iných ako mikropodniky, že uvedené finančné subjekty musia viesť záznamy o informáciách potrebných na vykonávanie osobitného posudzovania IKT rizika všetkých pôvodných IKT systémov uvedených v článku 8 ods. 7 nariadenia (EÚ) 2022/2554.

Článok 5
Postup v oblasti riadenia IKT aktív

1. Finančné subjekty vypracujú, zdokumentujú a vykonávajú postup v prípade riadenia IKT aktív.

2. V postupe riadenia IKT aktív uvedenom v odseku 1 sa stanovia kritériá na vykonávanie posudzovania kritickosti informačných aktív a IKT aktív podporujúcich obchodné funkcie. V uvedenom posúdení sa zohľadnia tieto aspekty:

a) IKT riziko súvisiace s uvedenými obchodnými funkciami a ich závislosti od informačných aktív alebo IKT aktív;

b) ako by strata dôvernosti, integrity a dostupnosti takýchto informačných aktív a IKT aktív ovplyvnila obchodné procesy a činnosti finančných subjektov.

ODDIEL 4
ŠIFROVANIE A KRYPTOGRAFIA

Článok 6
Šifrovanie a kryptografické kontroly

1. V rámci svojich politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú politiku v oblasti šifrovania a kryptografických kontrol.

2. Finančné subjekty navrhujú politiku v oblasti šifrovania a kryptografických kontrol uvedenú v odseku 1 na základe výsledkov schválenej klasifikácie údajov a posudzovania IKT rizika. Uvedená politika obsahuje pravidlá pre všetky tieto oblasti:

a) šifrovanie údajov v pokoji a pri prenose;

b) v prípade potreby šifrovanie údajov pri ich používaní;

c) šifrovanie interných sieťových pripojení a prevádzky s externými stranami;

d) riadenie šifrovacích kľúčov uvedené v článku 7 stanovením pravidiel správneho používania, ochrany a životného cyklu šifrovacích kľúčov.

Na účely písmena b) platí, že ak šifrovanie údajov pri používaní nie je možné, finančné subjekty spracúvajú údaje pri používaní v oddelenom a chránenom prostredí alebo prijmú rovnocenné opatrenia na zabezpečenie dôvernosti, integrity, pravosti a dostupnosti údajov.

3. Finančné subjekty zahrnú do politiky v oblasti šifrovania a kryptografických kontrol uvedenej v odseku 1 kritériá výberu kryptografických techník a postupov používania, pričom zohľadnia popredné postupy a normy vymedzené v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012 a klasifikáciu príslušných IKT aktív stanovenú v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554. Finančné subjekty, ktoré nemôžu dodržiavať popredné postupy alebo normy či používať najspoľahlivejšie techniky, prijmú zmierňujúce a monitorovacie opatrenia, ktorými sa zabezpečí odolnosť voči kybernetickým hrozbám.

4. Finančné subjekty zahrnú do politiky v oblasti šifrovania a kryptografických kontrol uvedenej v odseku 1 ustanovenia o aktualizácii alebo prípadne zmene kryptografickej technológie, a to na základe vývoja v oblasti kryptoanalýzy. Týmito aktualizáciami alebo zmenami sa zabezpečí, aby kryptografická technológia bola neustále odolná voči kybernetickým hrozbám, ako sa vyžaduje v článku 10 ods. 2 písm. a). Finančné subjekty, ktoré nemôžu aktualizovať alebo zmeniť kryptografickú technológiu, prijmú zmierňujúce a monitorovacie opatrenia, ktorými sa zabezpečí odolnosť voči kybernetickým hrozbám.

5. Finančné subjekty zahrnú do politiky v oblasti šifrovania a kryptografických kontrol uvedenej v odseku 1 požiadavku zaznamenávať prijatie zmierňujúcich a monitorovacích opatrení prijatých v súlade s odsekmi 3 a 4 a poskytovať k tomu odôvodnené vysvetlenie.

Článok 7
Riadenie šifrovacích kľúčov

1. Finančné subjekty zahrnú do politiky v oblasti riadenia šifrovacích kľúčov uvedenej v článku 6 ods. 2 písm. d) požiadavky na riadenie šifrovacích kľúčov počas ich celého životného cyklu vrátane generovania, obnovovania, uchovávania, zálohovania, archivovania, vyhľadávania, prenosu, zrušenia, odnímania a zničenia uvedených šifrovacích kľúčov.

2. Finančné subjekty identifikujú a vykonávajú kontroly na ochranu šifrovacích kľúčov počas celého ich životného cyklu pred stratou, neoprávneným prístupom, zverejnením a zmenou. Finančné subjekty navrhujú uvedené kontroly na základe výsledkov schválenej klasifikácie údajov a posudzovania IKT rizika.

3. Finančné subjekty vypracujú a vykonávajú metódy na nahradenie šifrovacích kľúčov v prípade straty alebo ak sú tieto kľúče ohrozené alebo poškodené.

4. Finančné subjekty vytvoria a vedú register pre všetky certifikáty a zariadenia na ukladanie certifikátov aspoň pre IKT aktíva podporujúce kritické alebo dôležité funkcie. Finančné subjekty udržiavajú tento register v aktualizovanom stave.

5. Finančné subjekty zabezpečia urýchlené obnovenie certifikátov pred uplynutím ich platnosti.

ODDIEL 5
BEZPEČNOSŤ OPERÁCIÍ IKT

Článok 8
Politiky a postupy v prípade operácií IKT

1. V rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú politiky a postupy s cieľom riadiť operácie IKT. V týchto politikách a postupoch sa stanoví, ako finančné subjekty prevádzkujú, monitorujú, kontrolujú a obnovujú svoje IKT aktíva vrátane dokumentácie operácií IKT.

2. Politiky a postupy v prípade operácií IKT uvedené v odseku 1 obsahujú všetky tieto prvky:

   a) opis IKT aktív vrátane všetkých týchto prvkov:

      i) požiadavky týkajúce sa bezpečnej inštalácie, údržby, konfigurácie a deinštalácie IKT systému;

      ii) požiadavky týkajúce sa riadenia informačných aktív používaných IKT aktívami vrátane ich automatizovaného aj manuálneho spracovania a riešenia;

      iii) požiadavky týkajúce sa identifikácie a kontroly pôvodných IKT systémov;

   b) kontrola a monitorovanie IKT systémov vrátane všetkých týchto prvkov:

      i) zálohovanie a obnova požiadaviek na IKT systémy;

      ii) požiadavky na plánovanie, pričom sa zohľadňujú vzájomné závislosti medzi IKT systémami;

      iii) protokoly v prípade informácií o audítorskom zázname a systéme vedenia záznamov;

      iv) požiadavky na zabezpečenie toho, aby sa vykonávaním vnútorného auditu a iného testovania minimalizovalo narušenie obchodných operácií;

      v) požiadavky na oddelenie produkčných prostredí IKT od prostredí, v ktorých sa systémy IKT vyvíjajú a testujú, alebo od iných neprodukčných prostredí;

      vi) požiadavky na vykonávanie vývoja a testovania v prostrediach, ktoré sú oddelené od produkčného prostredia;

      vii) požiadavky na vykonávanie vývoja a testovania v produkčných prostrediach;

   c) riešenie chýb týkajúce sa IKT systémov vrátane všetkých týchto prvkov:

      i) postupy a protokoly na riešenie chýb;

ii) kontaktné osoby na vykonanie podpory a riešenie eskalácie vrátane kontaktných osôb externej podpory v prípade neočakávaných operačných alebo technických problémov;

iii) postupy reštartovania, návratu do pôvodného stavu a obnovy IKT systémov, ktoré sa majú použiť v prípade narušenia IKT systémov.

Na účely písmena b) bodu v) sa pri oddelení zohľadňujú všetky zložky daného prostredia vrátane účtov, údajov alebo pripojení, ako sa vyžaduje v článku 13 ods. 1 písm. a).

Na účely písmena b) bodu vii) sa v politikách a postupoch uvedených v odseku 1 stanoví, že prípady, v ktorých sa testovanie vykonáva v produkčnom prostredí, sú jasne identifikované, odôvodnené, majú obmedzené časové trvanie a sú schválené príslušnou funkciou v súlade s článkom 16 ods. 6. Finančné subjekty zabezpečia dostupnosť, dôvernosť, integritu a pravosť IKT systémov a produkčných údajov počas vývojových a testovacích činností v produkčnom prostredí.

Článok 9
Riadenie kapacít a výkonnosti

1. V rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú postupy riadenia kapacít a výkonnosti v súvislosti s týmito prvkami:

   a) identifikácia kapacitných požiadaviek ich IKT systémov;

   b) uplatňovanie optimalizácie zdrojov;

   c) postupy monitorovania na účely udržiavania a zlepšovania, pokiaľ ide o:

      i) dostupnosť údajov a IKT systémov;

      ii) efektívnosť IKT systémov;

      iii) predchádzanie nedostatku IKT kapacít.

2. Postupmi riadenia kapacít a výkonnosti uvedenými v odseku 1 sa zabezpečí, aby finančné subjekty prijali opatrenia, ktoré sú vhodné na zohľadnenie špecifík IKT systémov s dlhými alebo zložitými procesmi obstarávania alebo schvaľovania či IKT systémov, ktoré sú náročné na zdroje.

Článok 10
Riadenie zraniteľnosti a bezpečnostných záplat

1. V rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú postupy riadenia zraniteľnosti.

2. Postupmi riadenia zraniteľnosti uvedenými v odseku 1 sa:

   a) identifikujú a aktualizujú relevantné a dôveryhodné informačné zdroje na účely budovania a udržiavania povedomia o zraniteľných miestach;

   b) zabezpečuje vykonávanie automatizovaného skenovania zraniteľnosti a posudzovaní IKT aktív, pričom frekvencia a rozsah týchto činností

zodpovedajú klasifikácii stanovenej v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554 a celkovému rizikovému profilu IKT aktíva;

c) overuje, či:

i) externí poskytovatelia IKT služieb riešia zraniteľné miesta súvisiace s IKT službami poskytovanými finančnému subjektu;

ii) uvedení poskytovatelia služieb včas oznamujú finančnému subjektu aspoň kritické zraniteľné miesta, štatistické údaje a trendy;

d) sleduje používanie:

i) knižníc tretích strán vrátane knižníc s otvoreným zdrojovým kódom, ktoré sú využívané IKT službami podporujúcimi kritické alebo dôležité funkcie;

ii) IKT služieb, ktoré vyvinul samotný finančný subjekt alebo ktoré pre finančný subjekt osobitne prispôsobil či vyvinul externý poskytovateľ IKT služieb;

e) stanovujú postupy na zodpovedné zverejňovanie zraniteľných miest klientom, protistranám a verejnosti;

f) uprednostňuje zavedenie bezpečnostných záplat a iných zmierňujúcich opatrení na riešenie identifikovaných zraniteľných miest;

g) monitoruje a overuje náprava zraniteľných miest;

h) požaduje, aby sa všetky odhalené zraniteľné miesta ovplyvňujúce IKT systémy zaznamenávali a ich riešenia monitorovali.

Na účely písmena b) finančné subjekty vykonávajú automatizované skenovanie a posudzovanie zraniteľnosti IKT aktív v prípade IKT aktív podporujúcich kritické alebo dôležité funkcie aspoň raz týždenne.

Na účely písmena c) finančné subjekty požadujú, aby externí poskytovatelia IKT služieb preskúmali príslušné zraniteľné miesta, zistili základné príčiny a vykonali vhodné zmierňujúce opatrenia.

Na účely písmena d) finančné subjekty v náležitých prípadoch v spolupráci s externým poskytovateľom IKT služieb monitorujú verziu a možné aktualizácie knižníc tretích strán. V prípade IKT aktív alebo zložiek IKT aktív pripravených na použitie (off-the-shelf) a nadobudnutých a používaných pri prevádzke IKT služieb, ktoré nie sú určené na podporu kritických alebo dôležitých funkcií, finančné subjekty v čo najväčšej možnej miere sledujú využívanie knižníc tretích strán vrátane knižníc s otvoreným zdrojovým kódom.

Na účely písmena f) finančné subjekty zohľadňujú kritickosť zraniteľnosti, klasifikáciu stanovenú v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554 a rizikový profil IKT aktív ovplyvnených identifikovanými zraniteľnými miestami.

3. V rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú postupy riadenia bezpečnostných záplat.

4. Postupmi riadenia bezpečnostných záplat uvedenými v odseku 3 sa:

a) v čo najväčšej možnej miere identifikujú a vyhodnocujú dostupné softvérové a hardvérové bezpečnostné záplaty a aktualizácie prostredníctvom používania automatizovaných nástrojov;

b) identifikujú núdzové postupy na používanie bezpečnostných záplat a aktualizáciu IKT aktív;

c) testujú a zavádzajú softvérové a hardvérové bezpečnostné záplaty a aktualizácie uvedené v článku 8 ods. 2 písm. b) bodoch v), vi) a vii);

d) stanujú lehoty na inštaláciu softvérových a hardvérových bezpečnostných záplat a aktualizácií a eskalačné postupy, ak tieto lehoty nemožno dodržať.

Článok 11
Bezpečnosť údajov a systému

1. V rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT uvedených v článku 9 ods. 2 nariadenia (EÚ) 2022/2554 finančné subjekty vypracujú, zdokumentujú a vykonávajú postup v oblasti bezpečnosti údajov a systému.

2. Postup v oblasti bezpečnosti údajov a systému uvedený v odseku 1 obsahuje všetky tieto prvky týkajúce sa bezpečnosti údajov a IKT systému v súlade s klasifikáciou stanovenou v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554:

a) obmedzenia prístupu uvedené v článku 21 tohto nariadenia, ktoré podporujú požiadavky na ochranu pre každý stupeň utajenia;

b) identifikácia bezpečnej základnej konfigurácie v prípade IKT aktív, ktorou sa minimalizuje vystavenie týchto IKT aktív kybernetickým hrozbám, a opatrenia na pravidelné overovanie toho, či sú tieto základné konfigurácie účinne zavedené;

c) identifikácia bezpečnostných opatrení s cieľom zaistiť, aby sa do systémov IKT a koncových zariadení inštaloval len autorizovaný softvér;

d) identifikácia bezpečnostných opatrení proti škodlivým kódom;

e) identifikácia bezpečnostných opatrení na zabezpečenie toho, aby sa na prenos a uchovávanie údajov finančného subjektu používali len autorizované médiá na uchovávanie údajov, systémy a koncové zariadenia;

f) tieto požiadavky na zabezpečenie používania prenosných koncových zariadení a súkromných neprenosných koncových zariadení:

i) požiadavka na používanie riešenia v oblasti riadenia, pokiaľ ide o diaľkové riadenie koncových zariadení a diaľkový výmaz údajov finančného subjektu;

ii) požiadavka na používanie bezpečnostných mechanizmov, ktoré nemôžu zamestnanci alebo externí poskytovatelia IKT služieb neautorizovaným spôsobom zmeniť, odstrániť alebo obísť;

iii) požiadavka na používanie odstrániteľných pamäťových zariadení na záznam údajov len vtedy, ak sa zvyškové IKT riziko pohybuje v rámci úrovne tolerancie rizika finančného subjektu uvedenej v článku 3 ods. 1 písm. a);

g) postup bezpečného vymazania údajov, ktoré sa nachádzajú v priestoroch finančného subjektu alebo sú uložené externe, ktoré finančný subjekt už nemusí zhromažďovať ani uchovávať;

h) postup bezpečnej likvidácie alebo vyradenia z prevádzky pamäťových zariadení na záznam údajov, ktoré sa nachádzajú v priestoroch finančného subjektu alebo sú uložené externe a ktoré obsahujú dôverné informácie;

i) identifikácia a vykonávanie bezpečnostných opatrení, aby sa zabránilo strate a úniku údajov v prípade systémov a koncových zariadení;

j) vykonávanie bezpečnostných opatrení s cieľom zabezpečiť, aby telepráca a používanie súkromných koncových zariadení nemali nepriaznivý vplyv na bezpečnosť IKT finančného subjektu;

k) v prípade IKT aktív alebo služieb prevádzkovaných externým poskytovateľom IKT služieb identifikácia a vykonávanie požiadaviek na zachovanie digitálnej prevádzkovej odolnosti v súlade s výsledkami klasifikácie údajov a posudzovania IKT rizika.

Na účely písmena b) sa v bezpečnej základnej konfigurácii spomínanej v uvedenom písmene zohľadňujú popredné postupy a vhodné techniky stanovené v normách vymedzených v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012.

Na účely písmena k) finančné subjekty zohľadňujú tieto prvky:

a) vykonávanie nastavení odporúčaných predajcom, pokiaľ ide o prvky prevádzkované finančným subjektom;

b) jasné prideľovanie úloh a zodpovedností v oblasti informačnej bezpečnosti medzi finančným subjektom a externým poskytovateľom IKT služieb v súlade so zásadou plnej zodpovednosti finančného subjektu za jeho externého poskytovateľa IKT služieb, ako sa uvádza v článku 28 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, a v prípade finančných subjektov uvedených v článku 28 ods. 2 uvedeného nariadenia v súlade s politikou finančného subjektu týkajúcou sa využívania IKT služieb podporujúcich kritické alebo dôležité funkcie;

c) potreba zabezpečiť a zachovávať primerané kompetencie v rámci finančného subjektu v oblasti riadenia a bezpečnosti využívanej služby;

d) technické a organizačné opatrenia na minimalizáciu rizík súvisiacich s infraštruktúrou, ktorú využíva externý poskytovateľ IKT služieb pre svoje IKT služby, s prihliadnutím na popredné postupy a normy vymedzené v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012.

Článok 12
Vedenie záznamov

1. Finančné subjekty ako súčasť ochranných opatrení proti vniknutiu a zneužitiu údajov vypracujú, zdokumentujú a vykonávajú postupy, protokoly a nástroje vedenia záznamov.

2. Postupy, protokoly a nástroje v oblasti vedenia záznamov uvedené v odseku 1 obsahujú všetky tieto prvky:

a) identifikácia udalostí, ktoré sa majú zaznamenávať, obdobie uchovávania záznamových protokolov a opatrenia na zabezpečenie a spracovanie údajov

o záznamových protokoloch vzhľadom na účel, na ktorý sa záznamové protokoly vytvárajú;

b) zosúladenie úrovne podrobnosti záznamových protokolov s ich účelom a použitím, aby sa umožnilo účinné odhaľovanie anomálnych činností, ako sa uvádza v článku 24;

c) požiadavka na zaznamenávanie udalostí súvisiacich so všetkými týmito prvkami:

   i) kontrola logického a fyzického prístupu, ako sa uvádza v článku 21, a správa systému identifikačných dát;

   ii) riadenie kapacít;

   iii) riadenie zmien;

   iv) operácie IKT vrátane činností IKT systému;

   v) činnosti v oblasti sieťovej prevádzky vrátane výkonnosti siete IKT;

d) opatrenia na ochranu systémov vedenia záznamov a záznamových informácií pred neoprávnenou manipuláciou, vymazaním a neoprávneným prístupom v pokoji, pri prenose a v prípade potreby pri používaní;

e) opatrenia na zistenie zlyhania systémov vedenia záznamov;

f) bez toho, aby boli dotknuté akékoľvek uplatniteľné regulačné požiadavky podľa právnych predpisov Únie alebo vnútroštátneho práva, synchronizácia hodín každého IKT systému finančného subjektu na základe zdokumentovaného spoľahlivého zdroja referenčného času.

Na účely písmena a) finančné subjekty stanovia obdobie uchovávania, pričom zohľadnia obchodné ciele a ciele v oblasti informačnej bezpečnosti, dôvod zaznamenania udalosti do záznamových protokolov a výsledky posudzovania IKT rizika.

ODDIEL 6
BEZPEČNOSŤ SIETE

Článok 13
Riadenie bezpečnosti siete

1. Finančné subjekty ako súčasť záruk zaisťujúcich bezpečnosť sietí pred vniknutím a zneužitím údajov vypracujú, zdokumentujú a vykonávajú politiky, postupy, protokoly a nástroje riadenia bezpečnosti siete vrátane všetkých týchto prvkov:

   a) segregácia a segmentácia IKT systémov a sietí s prihliadnutím na:

      i) kritickosť alebo dôležitosť funkcie, ktorú tieto IKT systémy a siete podporujú;

      ii) klasifikácia stanovená v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554;

      iii) celkový rizikový profil IKT aktív využívajúcich tieto IKT systémy a siete;

   b) dokumentácia o všetkých sieťových pripojeniach a tokoch údajov finančného subjektu;

c) používanie samostatnej a špecializovanej siete na správu IKT aktív;

d) identifikácia a vykonávanie kontrol prístupu do siete s cieľom predchádzať pripojeniam všetkých neoprávnených zariadení alebo systémov alebo akéhokoľvek koncového bodu, ktoré nespĺňa bezpečnostné požiadavky finančného subjektu, do siete finančného subjektu a odhaľovať ich;

e) šifrovanie sieťových pripojení prechádzajúcich cez podnikové siete, verejné siete, domáce siete, externé siete a bezdrôtové siete pre používané komunikačné protokoly, pričom sa zohľadnia výsledky schválenej klasifikácie údajov, výsledky posudzovania IKT rizika a šifrovanie sieťových pripojení uvedené v článku 6 ods. 2;

f) navrhovanie sietí v súlade s bezpečnostnými požiadavkami v oblasti IKT stanovenými finančným subjektom s prihliadnutím na popredné postupy na zabezpečenie dôvernosti, integrity a dostupnosti siete;

g) zabezpečenie sieťovej prevádzky medzi vnútornými sieťami a internetom a inými externými pripojeniami;

h) identifikácia úloh, zodpovedností a krokov týkajúcich sa špecifikácie, vykonávania, schvaľovania, zmeny a preskúmania pravidiel firewallu a filtrov pripojení;

i) vykonávanie preskúmaní architektúry siete a koncepcie bezpečnosti siete raz ročne a pravidelne v prípade mikropodnikov s cieľom identifikovať potenciálne zraniteľné miesta;

j) v prípade potreby opatrenia na dočasnú izoláciu podsietí, sieťových prvkov a zariadení;

k) vykonávanie bezpečnej základnej konfigurácie všetkých sieťových prvkov a posilňovanie siete a sieťových zariadení v súlade so všetkými pokynmi pre predajcu, prípadne normami vymedzenými v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012, a poprednými postupmi;

l) postupy na obmedzenie, zablokovanie a ukončenie systémových a vzdialených spojení po určitom období nečinnosti;

m) v prípade zmlúv o sieťových službách:

   i) identifikácia a špecifikácia opatrení v oblasti IKT a informačnej bezpečnosti, úrovní služieb a požiadaviek na riadenie všetkých sieťových služieb;

   ii) či uvedené služby poskytuje vnútroskupinový poskytovateľ IKT služieb alebo externí poskytovatelia IKT služieb.

Na účely písmena h) finančné subjekty pravidelne vykonávajú preskúmanie pravidiel firewallu a filtrov pripojení v súlade s klasifikáciou stanovenou podľa článku 8 ods. 1 nariadenia (EÚ) 2022/2554 a celkovým rizikovým profilom dotknutých IKT systémov. V prípade IKT systémov, ktoré podporujú kritické alebo dôležité funkcie, finančné subjekty overujú primeranosť existujúcich pravidiel firewallu a filtrov pripojenia aspoň každých 6 mesiacov.

Článok 14
Zabezpečenie informácií pri prenose

1. Ako súčasť záruk na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov finančné subjekty vypracujú, zdokumentujú a vykonávajú politiky, postupy, protokoly a nástroje na ochranu informácií pri prenose. Finančné subjekty zabezpečia najmä všetky tieto prvky:

   a) dostupnosť, pravosť, integrita a dôvernosť údajov počas prenosu v sieti a stanovenie postupov na posudzovanie súladu s uvedenými požiadavkami;

   b) predchádzanie únikom údajov a ich odhaľovanie, ako aj zabezpečený prenos informácií medzi finančným subjektom a externými stranami;

   c) vykonávanie, dokumentácia a pravidelne preskúmanie požiadaviek na opatrenia na zachovanie dôvernosti alebo nezverejňovanie informácií, ktoré odrážajú potreby finančného subjektu na ochranu informácií v prípade zamestnancov finančného subjektu aj tretích strán.

2. Finančné subjekty navrhujú politiky, postupy, protokoly a nástroje na ochranu informácií počas prenosu uvedené v odseku 1 na základe výsledkov schválenej klasifikácie údajov a posudzovania IKT rizika.

ODDIEL 7
RIADENIE IKT PROJEKTU A ZMIEN

Článok 15
Riadenie IKT projektu

1. Ako súčasť záruk na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov finančné subjekty vypracujú, zdokumentujú a vykonávajú politiku riadenia IKT projektu.

2. V politike riadenia IKT projektu uvedenej v odseku 1 sa stanovujú prvky, ktorými sa zabezpečuje účinné riadenie IKT projektov súvisiacich s nadobudnutím, údržbou a prípadne vývojom IKT systémov finančného subjektu.

3. Politika riadenia IKT projektu uvedená v odseku 1 obsahuje všetky tieto prvky:

   a) ciele IKT projektu;

   b) riadenie IKT projektu vrátane úloh a zodpovedností;

   c) plánovanie, časový rámec a fázy IKT projektu;

   d) posúdenie rizika IKT projektu;

   e) príslušné čiastkové ciele;

   f) požiadavky na riadenie zmien;

   g) testovanie všetkých požiadaviek vrátane bezpečnostných požiadaviek a príslušný schvaľovací proces pri zavádzaní IKT systému v produkčnom prostredí.

4. Politikou riadenia IKT projektu uvedenou v odseku 1 sa zaistí bezpečné vykonávanie IKT projektu na základe poskytovania potrebných informácií a odborných znalostí z obchodnej oblasti alebo funkcií ovplyvnených IKT projektom.

5. V súlade s posúdením rizika IKT projektu uvedeným v odseku 3 písm. d) sa v politike riadenia IKT projektu uvedenej v odseku 1 stanoví, že zriadenie a pokrok IKT projektov, ktoré majú vplyv na kritické alebo dôležité funkcie finančného subjektu, a s nimi súvisiace riziká sa nahlasujú riadiacemu orgánu takto:

   a) jednotlivo alebo súhrnne v závislosti od významu a veľkosti IKT projektov;

   b) pravidelne a v prípade potreby na základe udalostí.

Článok 16
Nadobudnutie, vývoj a údržba IKT systémov

1. Ako súčasť záruk na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov finančné subjekty vypracujú, zdokumentujú a vykonávajú politiku, ktorou sa riadi nadobudnutie, vývoj a údržba IKT systémov. Touto politikou sa:

   a) identifikujú bezpečnostné postupy, ako aj metodiky týkajúce sa nadobúdania, vývoja a údržby IKT systémov;

   b) požaduje identifikácia týchto prvkov:

      i) technické špecifikácie a technické špecifikácie IKT v zmysle vymedzenia v článku 2 bodoch 4 a 5 nariadenia (EÚ) č. 1025/2012;

      ii) požiadavky týkajúce sa nadobudnutia, vývoja a údržby IKT systémov s osobitným zameraním na bezpečnostné požiadavky v oblasti IKT a na ich schválenie príslušnou obchodnou funkciou a vlastníkom IKT aktív v súlade s vnútornými mechanizmami správy a riadenia finančného subjektu;

   c) stanovujú opatrenia na zmiernenie rizika neúmyselnej zmeny IKT systémov alebo úmyselnej manipulácie s IKT systémami počas vývoja, údržby a zavádzania týchto IKT systémov v produkčnom prostredí.

2. Finančné subjekty vypracujú, zdokumentujú a vykonávajú postup nadobudnutia, vývoja a údržby IKT systémov na účely testovania a schvaľovania všetkých IKT systémov pred ich použitím a po údržbe v súlade s článkom 8 ods. 2 písm. b) bodmi v), vi) a vii). Úroveň testovania zodpovedá kritickosti dotknutých obchodných postupov a IKT aktív. Testovanie musí byť navrhnuté tak, aby sa overilo, či sú nové IKT systémy primerané na to, aby fungovali podľa plánu, a to vrátane overenia kvality softvéru vyvinutého interne.

   Centrálne protistrany popri požiadavkách stanovených v prvom pododseku v prípade potreby zapoja do navrhovania a vykonávania testovania uvedeného v prvom pododseku tieto subjekty:

   a) zúčtovacích členov a klientov;

   b) interoperabilné centrálne protistrany;

   c) iné zainteresované strany.

   Centrálne depozitáre cenných papierov popri požiadavkách stanovených v prvom pododseku v prípade potreby zapoja do navrhovania a vykonávania testovania uvedeného v prvom pododseku tieto subjekty:

   a) užívateľov;

   b) poskytovateľov kritických sieťových odvetví a kritických služieb;

c) iné centrálne depozitáre cenných papierov;

d) iné trhové infraštruktúry;

e) akékoľvek iné inštitúcie, v súvislosti s ktorými centrálne depozitáre cenných papierov identifikovali vo svojej politike kontinuity činností vzájomné závislosti.

3. Postup uvedený v odseku 2 obsahuje vykonávanie preskúmaní zdrojových kódov, ktoré sa vzťahujú na statické aj dynamické testovanie. Uvedené testovanie zahŕňa testovanie bezpečnosti systémov a aplikácií vystavených internetu v súlade s článkom 8 ods. 2 písm. b) bodmi v), vi) a vii). Finančné subjekty musia:

a) identifikovať a analyzovať zraniteľné miesta a anomálie v zdrojovom kóde;

b) prijať akčný plán na riešenie uvedených zraniteľných miest a anomálií;

c) monitorovať vykonávanie tohto akčného plánu.

4. Postup uvedený v odseku 2 obsahuje bezpečnostné testovanie softvérových balíkov najneskôr vo fáze integrácie v súlade s článkom 8 ods. 2 písm. b) bodmi v), vi) a vii).

5. V postupe uvedenom v odseku 2 sa stanoví, že:

a) neprodukčné prostredia uchovávajú len anonymizované, pseudonymizované alebo randomizované produkčné údaje;

b) finančné subjekty majú chrániť integritu a dôvernosť údajov v neprodukčných prostrediach.

6. Odchylne od odseku 5 sa v postupe uvedenom v odseku 2 môže stanoviť, že produkčné údaje sa uchovávajú len na osobitné testovacie prípady, a to na obmedzené časové obdobia a po schválení príslušnou funkciou, pričom takéto testovacie prípady sa nahlasujú funkcii riadenia IKT rizika.

7. Postup uvedený v odseku 2 obsahuje vykonávanie kontrol na ochranu integrity zdrojového kódu IKT systémov, ktoré vyvíja interný poskytovateľ IKT služieb alebo externý poskytovateľ IKT služieb a ktoré finančnému subjektu dodáva externý poskytovateľ IKT služieb.

8. V postupe uvedenom v odseku 2 sa stanoví, že proprietárny softvér a, ak je to možné, zdrojový kód, ktoré poskytujú externí poskytovatelia IKT služieb alebo ktoré pochádzajú z projektov s otvoreným zdrojovým kódom, sa majú analyzovať a testovať v súlade s odsekom 3 pred tým, ako dôjde k ich zavedeniu do produkčného prostredia.

9. Odseky 1 až 8 tohto článku sa uplatňujú aj na IKT systémy vyvinuté alebo spravované používateľmi mimo IKT funkcie, pričom sa používa prístup založený na riziku.

Článok 17
Riadenie zmien IKT

1. Ako súčasť záruk na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov finančné subjekty zahrnú do postupov riadenia zmien IKT uvedených v článku 9 ods. 4 písm. e) nariadenia (EÚ) 2022/2554, pokiaľ ide o všetky zmeny komponentov softvéru, hardvéru, firmvéru, systémov alebo bezpečnostných parametrov, všetky tieto prvky:

a) overenie toho, či boli splnené bezpečnostné požiadavky v oblasti IKT;

b) mechanizmy na zabezpečenie nezávislosti funkcií, ktoré schvaľujú zmeny, ako aj funkcií, ktoré sú zodpovedné za podávanie žiadostí o uvedené zmeny a ich vykonávanie;

c) jasný opis úloh a povinností s cieľom zabezpečiť, aby:

   i) zmeny boli bližšie stanovené a plánované;

   ii) bolo navrhnuté primerané prechodné obdobie;

   iii) zmeny boli otestované a sfinalizované kontrolovane;

   iv) existovalo účinné zabezpečenie kvality;

d) dokumentácia a nahlasovanie podrobností o zmene vrátane:

   i) účelu a rozsahu zmeny;

   ii) časového rámca vykonávania zmeny;

   iii) očakávaného výsledku;

e) identifikácia núdzových postupov a zodpovedností vrátane postupov a zodpovedností za zrušenie zmien alebo obnovenie stavu pred zmenami, ktoré neboli úspešne vykonané;

f) postupy, protokoly a nástroje na riadenie núdzových zmien, ktoré poskytujú primerané záruky;

g) postupy na dokumentovanie, prehodnotenie, posudzovanie a schvaľovanie núdzových zmien po ich vykonaní vrátane dočasných riešení a bezpečnostných záplat;

h) identifikácia potenciálneho vplyvu zmeny na existujúce bezpečnostné opatrenia v oblasti IKT a posúdenie toho, či si takáto zmena vyžaduje prijatie dodatočných bezpečnostných opatrení v oblasti IKT.

2. Po významných zmenách vo svojich IKT systémoch centrálne protistrany a centrálne depozitáre cenných papierov podrobia svoje IKT systémy prísnemu testovaniu formou simulácie stresových podmienok.

Centrálne protistrany v prípade potreby zapoja do navrhovania a vykonávania testovania uvedeného v prvom pododseku tieto subjekty:

a) zúčtovacích členov a klientov;

b) interoperabilné centrálne protistrany;

c) iné zainteresované strany.

Centrálne depozitáre cenných papierov v prípade potreby zapoja do navrhovania a vykonávania testovania uvedeného v prvom pododseku tieto subjekty:

a) užívateľov;

b) poskytovateľov kritických sieťových odvetví a kritických služieb;

c) iné centrálne depozitáre cenných papierov;

d) iné trhové infraštruktúry;

e) akékoľvek iné inštitúcie, v súvislosti s ktorými centrálne depozitáre cenných papierov identifikovali vo svojej politike kontinuity činností v oblasti IKT vzájomné závislosti.

ODDIEL 8

Článok 18
Fyzická a environmentálna bezpečnosť

1. Ako súčasť záruk na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov finančné subjekty stanovia, zdokumentujú a vykonávajú politiku fyzickej a environmentálnej bezpečnosti. Finančné subjekty navrhujú uvedenú politiku vzhľadom na panorámu kybernetických hrozieb v súlade s klasifikáciou stanovenou podľa článku 8 ods. 1 nariadenia (EÚ) 2022/2554 a so zreteľom na celkový rizikový profil IKT aktív a dostupných informačných aktív.

2. Politika fyzickej a environmentálnej bezpečnosti uvedená v odseku 1 obsahuje všetky tieto prvky:

   a) odkaz na oddiel politiky v oblasti kontroly práv na riadenie prístupu uvedenú v článku 21 ods. 1 písm. g);

   b) opatrenia na ochranu priestorov, dátových centier finančného subjektu, ako aj citlivých určených oblastí identifikovaných finančným subjektom, v ktorých sa nachádzajú IKT aktíva a informačné aktíva, pred útokmi, nehodami a environmentálnymi hrozbami a nebezpečenstvami;

   c) opatrenia na zabezpečenie IKT aktív v priestoroch finančného subjektu aj mimo neho, pričom sa zohľadňujú výsledky posudzovania IKT rizika súvisiaceho s príslušnými IKT aktívami;

   d) opatrenia na zabezpečenie dostupnosti, pravosti, integrity a dôvernosti IKT aktív, informačných aktív a zariadení na kontrolu fyzického prístupu finančného subjektu prostredníctvom primeranej údržby;

   e) opatrenia na zachovanie dostupnosti, pravosti, integrity a dôvernosti údajov vrátane týchto prvkov:

      i) jednoznačná administratívna politika pre dokumenty v papierovej forme;

      ii) politika čistej obrazovky pre zariadenia na spracúvanie informácií.

   Na účely písmena b) zodpovedajú opatrenia na ochranu pred environmentálnymi hrozbami a nebezpečenstvami významu priestorov, dátových centier, citlivých určených oblastí a kritickosti operácií alebo IKT systémov, ktoré sa v nich nachádzajú.

   Na účely písmena c) politika fyzickej a environmentálnej bezpečnosti uvedená v odseku 1 obsahuje opatrenia na zabezpečenie primeranej ochrany aktív IKT nachádzajúcich sa bez dozoru.

Kapitola II
POLITIKA ĽUDSKÝCH ZDROJOV A KONTROLA PRÍSTUPU

Článok 19
Politika ľudských zdrojov

Finančné subjekty zahrnú do svojej politiky ľudských zdrojov alebo iných príslušných politík všetky tieto prvky súvisiace s bezpečnosťou IKT:

a) identifikácia a prideľovanie všetkých osobitných povinností v oblasti bezpečnosti IKT;

b) požiadavky na zamestnancov finančného subjektu a externých poskytovateľov IKT služieb, ktorí používajú IKT aktíva finančného subjektu alebo k nim majú prístup, zamerané na cieľ:

   i) byť informovaný o politikách, postupoch a protokoloch finančného subjektu v oblasti bezpečnosti IKT a dodržiavať ich;

   ii) poznať kanály nahlasovania zavedené finančným subjektom na odhaľovanie anomálneho správania vrátane prípadných kanálov nahlasovania vytvorených v súlade so smernicou Európskeho parlamentu a Rady (EÚ) 2019/1937[10];

   iii) vrátiť finančnému subjektu po skončení pracovného pomeru zamestnancov všetky IKT aktíva a hmotné informačné aktíva, ktoré majú v držbe a ktoré patria finančnému subjektu.

Článok 20
Správa systému identifikačných dát

1. Ako súčasť svojej kontroly práv na riadenie prístupu finančné subjekty vypracujú, zdokumentujú a vykonávajú politiky a postupy riadenia systému identifikačných dát, ktoré zabezpečujú jedinečnú identifikáciu a autentifikáciu fyzických osôb a systémov, ktoré majú prístup k informáciám finančných subjektov, s cieľom umožniť prideľovanie prístupových práv používateľov v súlade s článkom 21.

2. Politiky a postupy riadenia systému identifikačných dát uvedené v odseku 1 obsahujú všetky tieto prvky:

   a) pridelenie jedinečnej totožnosti zodpovedajúcej jedinečnému používateľskému účtu bez toho, aby bol dotknutý článok 21 ods. 1 písm. c), každému zamestnancovi finančného subjektu alebo všetkým zamestnancom externých poskytovateľov IKT služieb, ktorí majú prístup k informačným aktívam a IKT aktívam finančného subjektu;

   b) proces riadenia životného cyklu v prípade totožností a účtov, ktorými sa riadi vytváranie, zmena, preskúmanie a aktualizácia, dočasná deaktivácia a ukončenie všetkých účtov.

[10] Smernica Európskeho parlamentu a Rady (EÚ) 2019/1937 z 23. októbra 2019 o ochrane osôb, ktoré nahlasujú porušenia práva Únie (Ú. v. EÚ L 305 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

Na účely písmena a) finančné subjekty vedú záznamy o všetkých prideleniach totožnosti. Uvedené záznamy sa uchovávajú po reorganizácii finančného subjektu alebo po skončení zmluvného vzťahu bez toho, aby boli dotknuté požiadavky na uchovávanie stanovené v uplatniteľnom práve Únie a vo vnútroštátnom práve.

Na účely písmena b) finančné subjekty, ak je to možné a vhodné, zavedú automatizované riešenia pre proces riadenia systému identifikačných dát počas životného cyklu.

Článok 21
Kontrola prístupu

Finančné subjekty v rámci svojej kontroly práv na riadenie prístupu vypracujú, zdokumentujú a vykonávajú politiku, ktorá obsahuje všetky tieto prvky:

a) prideľovanie prístupových práv k aktívam IKT na základe zásady potreby poznať (need-to-know), zásady potreby používať (need-to-use) a zásady minimálneho privilégia (least privilege principle), a to aj v prípade vzdialeného a núdzového prístupu;

b) segregácia povinností určených na zabránenie neoprávnenému prístupu ku kritickým údajom alebo na zabránenie prideľovaniu kombinácií prístupových práv, ktoré sa môžu použiť na obchádzanie kontrol;

c) ustanovenie o zodpovednosti používateľa tým, že sa v čo najväčšej možnej miere obmedzí používanie generických a spoločných používateľských účtov a zabezpečí sa, aby boli používatelia vždy identifikovateľní, pokiaľ ide o činnosti, ktoré v IKT systémoch vykonávajú;

d) ustanovenie o obmedzeniach prístupu k IKT aktívam, v ktorom sa stanovujú kontroly a nástroje na zabránenie neoprávnenému prístupu;

e) postupy riadenia účtov na účely udeľovania, zmeny alebo odoberania prístupových práv k používateľským a generickým účtom vrátane generických správcovských účtov, vrátane ustanovení o všetkých týchto prvkoch:

   i) prideľovanie úloh a zodpovedností za udeľovanie, preskúmavanie a odoberanie prístupových práv;

   ii) prideľovanie privilegovaného, núdzového a správcovského prístupu na základe potreby používať (need-to-use) alebo na *ad hoc* základe pre všetky IKT systémy;

   iii) odobratie prístupových práv bez zbytočného odkladu po skončení pracovného pomeru, alebo ak prístup už nie je potrebný;

   iv) aktualizácia prístupových práv, ak sú potrebné zmeny, a to aspoň raz ročne v prípade všetkých IKT systémov iných ako IKT systémy podporujúce kritické alebo dôležité funkcie a aspoň každých 6 mesiacov v prípade IKT systémov podporujúcich kritické alebo dôležité funkcie;

f) metódy autentifikácie vrátane všetkých týchto prvkov:

   i) používanie metód autentifikácie zodpovedajúcich klasifikácii stanovenej v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554 a celkovému rizikovému profilu IKT aktív a s prihliadnutím na popredné postupy;

ii) používanie silných metód autentifikácie v súlade s poprednými postupmi a technikami v prípade vzdialeného prístupu do siete finančného subjektu, privilegovaného prístupu, prístupu k IKT aktívam podporujúcim kritické alebo dôležité funkcie alebo IKT aktívam, ktoré sú verejne prístupné;

g) opatrenia na kontrolu fyzického prístupu vrátane týchto prvkov:

i) identifikácia a vedenie záznamov o fyzických osobách, ktoré majú povolenie na prístup do priestorov, do dátových centier a citlivých určených oblastí identifikovaných finančným subjektom, v ktorých majú sídlo IKT a informačné aktíva;

ii) udeľovanie fyzických prístupových práv ku kritickým IKT aktívam len oprávneným osobám v súlade so zásadou potreba poznať (need-to-know) a zásadou minimálneho privilégia a na *ad hoc* základe;

iii) monitorovanie fyzického prístupu do priestorov, do dátových centier a citlivých určených oblastí identifikovaných finančným subjektom, v ktorých majú sídlo IKT a informačné aktíva alebo oboje;

iv) preskúmanie fyzických prístupových práv na zabezpečenie urýchleného odobratia nepotrebných prístupových práv.

Na účely písmena e) bodu i) finančné subjekty stanovia obdobie uchovávania, pričom zohľadnia obchodné ciele a ciele v oblasti informačnej bezpečnosti, dôvody zaznamenania udalosti do záznamových protokolov a výsledky posudzovania IKT rizika.

Na účely písmena e) bodu ii) finančné subjekty podľa možnosti používajú na plnenie administratívnych úloh týkajúcich sa IKT systémov osobitné účty. Ak je to uskutočniteľné a vhodné, finančné subjekty zavedú na riadenie privilegovaného prístupu automatizované riešenia.

Na účely písmena g) bodu i) zodpovedá identifikácia a vedenie záznamov významu priestorov, dátových centier, citlivých určených oblastí a kritickosti operácií alebo IKT systémov, ktoré sa v nich nachádzajú.

Na účely písmena g) bodu iii) zodpovedá monitorovanie klasifikácii stanovenej v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2022/2554 a kritickosti oblasti, do ktorej sa pristupuje.

KAPITOLA III
ODHAĽOVANIE INCIDENTOV SÚVISIACICH S IKT A REAKCIA NA NE

Článok 22
Politika riadenia incidentov súvisiacich s IKT

Ako súčasť mechanizmov na odhaľovanie anomálnych činností vrátane problémov s výkonnosťou siete IKT a incidentov súvisiacich s IKT finančné subjekty vypracujú, zdokumentujú a vykonávajú politiku v oblasti incidentov súvisiacich s IKT, prostredníctvom ktorej vykonávajú tieto činnosti:

a) dokumentácia procesu riadenia incidentov súvisiacich s IKT uvedeného v článku 17 nariadenia (EÚ) 2022/2554;

b) zostavenie zoznamu príslušných kontaktných osôb s internými funkciami a externými zainteresovanými stranami, ktoré sú priamo zapojené do bezpečnosti operácií IKT, a to aj pokiaľ ide o tieto prvky:

i) odhaľovanie a monitorovanie kybernetických hrozieb;

ii) odhaľovanie anomálnych činností;

iii) riadenie zraniteľnosti;

c) vytvorenie, vykonávanie a prevádzka technických, organizačných a prevádzkových mechanizmov na podporu procesu riadenia incidentov súvisiacich s IKT vrátane mechanizmov umožňujúcich urýchlené odhalenie anomálnych činností a správania v súlade s článkom 23 tohto nariadenia;

d) uchovávanie všetkých dôkazov týkajúcich sa incidentov súvisiacich s IKT počas obdobia, ktoré nie je dlhšie, ako je potrebné na účely, na ktoré sa údaje zhromažďujú, zodpovedá kritickosti ovplyvnených obchodných funkcií, podporných procesov, IKT aktív a informačných aktív v súlade s {článkom [15] delegovaného nariadenia Komisie (EÚ) [...]/[...] [delegované nariadenie Komisie o klasifikácii incidentov súvisiacich s IKT]}[11] a s akoukoľvek uplatniteľnou požiadavkou na uchovávanie podľa právnych predpisov Únie;

e) vytvorenie a zavedenie mechanizmov na analýzu významných alebo opakujúcich sa incidentov a modelov súvisiacich s IKT, pokiaľ ide o počet a výskyt incidentov súvisiacich s IKT.

Na účely písmena d) finančné subjekty uchovávajú dôkazy uvedené v uvedenom písmene bezpečne.

Článok 23

Odhaľovanie anomálnych činností, kritériá na odhaľovanie incidentov súvisiacich s IKT a reakcia na ne

1. Finančné subjekty stanovia jasné úlohy a povinnosti na účinné odhaľovanie incidentov a anomálnych činnosti súvisiacich s IKT a reakciu na ne.

2. Mechanizmus na urýchlené odhaľovanie anomálnych činností vrátane problémov s výkonnosťou siete IKT a incidentov súvisiacich s IKT, ako sa uvádza v článku 10 ods. 1 nariadenia (EÚ) 2022/2554, musí finančným subjektom umožňovať, aby vykonávali tieto činnosti:

a) zhromažďovať, monitorovať a analyzovať všetky tieto prvky:

i) interné a externé faktory vrátane aspoň záznamových protokolov zhromaždených v súlade s článkom 12 tohto nariadenia, informácií z obchodných a IKT funkcií a akýchkoľvek problémov nahlásených používateľmi finančného subjektu;

ii) potenciálne interné a externé kybernetické hrozby, pričom sa zohľadnia scenáre, ktoré bežne používajú aktéri hrozby, a scenáre, ktoré sú založené na činnosti spravodajských informácií o hrozbách;

iii) oznámenie incidentu súvisiaceho s IKT zo strany externého poskytovateľa IKT služieb finančného subjektu, ktorý bol zistený v IKT systémoch a sieťach externého poskytovateľa IKT služieb a ktorý môže ovplyvniť finančný subjekt;

[11] [Úrad pre publikácie: vložte odkaz a názov tohto delegovaného nariadenia Komisie].

b) identifikácia anomálnych činností a správania, ako aj zavedenie nástrojov vytvárajúcich varovania v prípade anomálnych činností a správania, a to aspoň v prípade IKT aktív a informačných aktív podporujúcich kritické alebo dôležité funkcie;

c) určenie priorít v prípade varovaní uvedených v písmene b) s cieľom umožniť riadenie zistených incidentov súvisiacich s IKT v rámci očakávaného času riešenia stanoveného finančnými subjektmi, a to počas pracovného času aj mimo neho;

d) automatické alebo manuálne zaznamenávanie, analýza a vyhodnocovanie všetkých relevantných informácií o všetkých anomálnych činnostiach a správaní.

Na účely písmena b) nástroje uvedené v uvedenom písmene obsahujú nástroje, ktoré poskytujú automatizované varovania na základe vopred vymedzených pravidiel na identifikáciu anomálií ovplyvňujúcich úplnosť a integritu zdrojov údajov alebo zhromažďovania záznamových protokolov.

3. Finančné subjekty chránia každý záznam o anomálnych činnostiach pred manipuláciou a neoprávneným prístupom v pokoji, pri prenose a v prípade potreby pri používaní.

4. Finančné subjekty vedú záznamy o všetkých relevantných informáciách o každej odhalenej anomálnej činnosti, ktoré umožňujú:

a) identifikáciu dátumu a času výskytu anomálnej činnosti;

b) identifikáciu dátumu a času odhalenia anomálnej činnosti;

c) identifikáciu typu anomálnej činnosti.

5. Finančné subjekty pri spustení procesov odhaľovania incidentov súvisiacich s IKT a reakciách na ne uvedených v článku 10 ods. 2 nariadenia (EÚ) 2022/2554 zohľadňujú všetky tieto kritériá:

a) indície, že v IKT systéme alebo sieti sa mohla vykonávať nekalá činnosť alebo že takýto IKT systém alebo sieť mohli byť napadnuté;

b) straty údajov zistené v súvislosti s dostupnosťou, pravosťou, integritou a dôvernosťou údajov;

c) zistený nepriaznivý vplyv na transakcie a operácie finančného subjektu;

d) nedostupnosť IKT systémov a siete.

6. Na účely odseku 5 finančné subjekty zohľadňujú aj kritickosť ovplyvnených služieb.

KAPITOLA IV
RIADENIE KONTINUITY ČINNOSTÍ V OBLASTI IKT

Článok 24
Zložky politiky kontinuity činností v oblasti IKT

1. Finančné subjekty zahrnú do svojej politiky kontinuity činností v oblasti IKT uvedenej v článku 11 ods. 1 nariadenia (EÚ) 2022/2554 všetky tieto prvky:

a) opis týchto prvkov:

i) ciele politiky kontinuity činností v oblasti IKT vrátane vzájomného vzťahu medzi IKT a celkovou kontinuitou činností a s prihliadnutím na výsledky analýzy vplyvu na svoje činnosti (BIA) uvedenej v článku 11 ods. 5 nariadenia (EÚ) 2022/2554;

ii) rozsah opatrení, plánov, postupov a mechanizmov na zabezpečenie kontinuity činností v oblasti IKT vrátane obmedzení a vylúčení;

iii) časový rámec, na ktorý sa majú vzťahovať opatrenia, plány, postupy a mechanizmy na zabezpečenie kontinuity činností v oblasti IKT;

iv) kritériá na aktiváciu a deaktiváciu plánov na zabezpečenie kontinuity činností v oblasti IKT, plánov reakcie a obnovy v oblasti IKT a plánov krízovej komunikácie;

b) ustanovenia týkajúce sa týchto činností:

i) správa a riadenie a organizácia na vykonávanie politiky kontinuity činností v oblasti IKT vrátane úloh, zodpovedností a eskalačných postupov, ktorými sa zabezpečí dostupnosť dostatočných zdrojov;

ii) zosúladenie medzi plánmi na zabezpečenie kontinuity činností v oblasti IKT a celkovými plánmi na zabezpečenie kontinuity činností, pokiaľ ide aspoň o všetky tieto aspekty:

(1) potenciálne scenáre zlyhania vrátane scenárov uvedených v článku 26 ods. 2 tohto nariadenia;

(2) ciele obnovy, v ktorých sa bližšie spresňuje, že finančný subjekt musí byť schopný obnoviť operácie svojich kritických alebo dôležitých funkcií po narušeniach v rámci časového cieľa obnovy a cieľa bodu obnovy;

iii) vypracovanie plánov na zabezpečenie kontinuity činností v oblasti IKT v prípade závažných narušení činnosti ako súčasť uvedených plánov a prioritizácia opatrení na zabezpečenie kontinuity činností v oblasti IKT s využitím prístupu založeného na riziku;

iv) vypracovanie, testovanie a preskúmanie plánov reakcie a obnovy v oblasti IKT v súlade s článkami 25 a 26 tohto nariadenia;

v) preskúmanie účinnosti zavedených opatrení, plánov, postupov a mechanizmov na zabezpečenie kontinuity činností v oblasti IKT v súlade s článkom 26 tohto nariadenia;

vi) zosúladenie politiky kontinuity činností v oblasti IKT s týmito prvkami:

(1) komunikačná politika uvedená v článku 14 ods. 2 nariadenia (EÚ) 2022/2554;

(2) opatrenia v oblasti komunikácie a krízového riadenia uvedené v článku 11 ods. 2 písm. e) nariadenia (EÚ) 2022/2554.

2. Popri požiadavkách uvedených v odseku 1 centrálne protistrany zabezpečia, aby ich politika kontinuity činností v oblasti IKT:

a) obsahovala maximálny čas obnovy v prípade ich kritických funkcií, ktorý nie je dlhší ako 2 hodiny;

b) zohľadňovala externé prepojenia a vzájomné závislosti v rámci finančných infraštruktúr vrátane obchodných miest zúčtovávaných centrálnou protistranou, zúčtovacích systémov cenných papierov a platobných systémov, ako aj úverových inštitúcií používaných centrálnou protistranou alebo prepojenou centrálnou protistranou;

c) vyžadovala zavedenie týchto opatrení:

i) zabezpečenie kontinuity kritických alebo dôležitých funkcií centrálnej protistrany na základe scenárov katastrof;

ii) udržiavanie sekundárneho miesta spracúvania, ktoré má kapacitu zabezpečiť kontinuitu kritických alebo dôležitých funkcií centrálnej protistrany identických s primárnym miestom;

iii) udržiavanie alebo poskytovanie okamžitého prístupu k sekundárnemu obchodnému miestu s cieľom umožniť zamestnancom zabezpečiť kontinuitu služby, ak primárne miesto podnikania nie je k dispozícii;

iv) zohľadnenie potreby ďalších miest spracovania, najmä ak rozmanitosť rizikových profilov primárneho a sekundárneho miesta neposkytuje dostatočnú istotu, že ciele kontinuity podnikateľskej činnosti centrálnej protistrany budú splnené v prípade všetkých scenárov.

Na účely písmena a) centrálne protistrany za každých okolností dokončia postupy a platby vykonávané na konci dňa v požadovaný čas a deň.

Na účely písmena c) bodu i) sa opatreniami uvedenými v uvedenom písmene rieši dostupnosť primeraných ľudských zdrojov, maximálny výpadok kritických funkcií a prechod na sekundárne miesto a jeho obnova.

Na účely písmena c) bodu ii) musí mať sekundárne miesto spracúvania uvedené v tomto písmene geografický rizikový profil, ktorý sa odlišuje od profilu primárneho miesta.

3. Popri požiadavkách uvedených v odseku 1 centrálne protistrany zabezpečia, aby ich politika kontinuity činností v oblasti IKT:

a) zohľadňovala všetky prepojenia a vzájomné závislosti s používateľmi, poskytovateľmi kritických sieťových odvetví a kritických služieb, inými centrálnymi depozitármi cenných papierov a inými trhovými infraštruktúrami;

b) vyžadovala, aby sa opatreniami na zabezpečenie kontinuity činností v oblasti IKT zaistilo, že časový cieľ obnovy kritických alebo dôležitých funkcií nebude dlhší ako 2 hodiny.

4. Popri požiadavkách uvedených v odseku 1 obchodné miesta zaistia, aby ich politika kontinuity činností v oblasti IKT zabezpečila tieto aspekty:

a) obchodovanie sa môže obnoviť do dvoch hodín alebo takmer do dvoch hodín po rušivom incidente;

b) maximálne množstvo údajov, ktoré možno stratiť z akejkoľvek IT služby obchodného miesta po rušivom incidente, sa blíži k nule.

Článok 25
Testovanie plánov kontinuity činností v oblasti IKT

1. Pri testovaní plánov kontinuity činností v oblasti IKT v súlade s článkom 11 ods. 6 nariadenia (EÚ) 2022/2554 finančné subjekty zohľadňujú analýzu vplyvu na svoje činnosti (BIA) a posudzovanie IKT rizika uvedené v článku 3 ods. 1 písm. b) tohto nariadenia.

2. Finančné subjekty testovaním svojich plánov kontinuity činností v oblasti IKT uvedených v odseku 1 posúdia, či dokážu zabezpečiť kontinuitu svojich kritických alebo dôležitých funkcií. Toto testovanie musí:

   a) byť vykonávané na základe testovacích scenárov, ktoré simulujú potenciálne narušenia vrátane primeraného súboru závažných, ale realistických scenárov;

   b) v prípade potreby obsahovať testovanie IKT služieb poskytovaných externými poskytovateľmi IKT služieb;

   c) v prípade finančných subjektov iných než mikropodniky, ako sa uvádza v článku 11 ods. 6 druhom pododseku nariadenia (EÚ) 2022/2554, obsahovať scenáre prepnutia medzi primárnou infraštruktúrou IKT a redundantnou kapacitou, zálohami a redundantnými zariadeniami;

   d) byť navrhnuté tak, aby sa spochybnili predpoklady, na ktorých sú založené plány na zabezpečenie kontinuity činností vrátane mechanizmov správy a riadenia a plánov krízovej komunikácie;

   e) obsahovať postupy na overovanie schopnosti zamestnancov finančných subjektov, externých poskytovateľov IKT služieb, IKT systémov a IKT služieb primerane reagovať na scenáre náležite zohľadnené v súlade s článkom 26 ods. 2.

   Na účely písmena a) finančné subjekty do testovania vždy zahrnú scenáre zvažované pri vypracúvaní plánov kontinuity činností.

   Na účely písmena b) finančné subjekty náležite zvážia scenáre spojené s platobnou neschopnosťou alebo zlyhaniami externých poskytovateľov IKT služieb alebo súvisiace s politickými rizikami v jurisdikciách externých poskytovateľov IKT služieb, ak je to relevantné.

   Na účely písmena c) sa testovaním overí, či je možné primerane vykonávať aspoň kritické alebo dôležité funkcie počas dostatočne dlhého časového obdobia a či je možné obnoviť normálne fungovanie.

3. Popri požiadavkách uvedených v odseku 2 centrálne protistrany zapoja do testovania svojich plánov kontinuity činností v oblasti IKT uvedených v odseku 1 tieto subjekty:

   a) zúčtovacích členov;

   b) externých poskytovateľov;

   c) príslušné inštitúcie vo finančnej infraštruktúre, v súvislosti s ktorými centrálne protistrany identifikovali vo svojich politikách kontinuity činností vzájomné závislosti.

4. Popri požiadavkách uvedených v odseku 2 centrálne depozitáre cenných papierov zapoja do testovania svojich plánov kontinuity činností v oblasti IKT uvedených v odseku 1 prípadne tieto subjekty:

a) používateľov centrálnych depozitárov cenných papierov;

b) poskytovateľov kritických sieťových odvetví a kritických služieb;

c) iné centrálne depozitáre cenných papierov;

d) iné trhové infraštruktúry;

e) akékoľvek iné inštitúcie, v súvislosti s ktorými centrálne depozitáre cenných papierov identifikovali vo svojej politike kontinuity činností vzájomné závislosti.

5. Finančné subjekty zdokumentujú výsledky testovania uvedeného v odseku 1. Všetky zistené nedostatky vyplývajúce z tohto testovania sa analyzujú, riešia a oznamujú riadiacemu orgánu.

Článok 26
Plány reakcie a obnovy v oblasti IKT

1. Pri vypracúvaní plánov reakcie a obnovy v oblasti IKT uvedených v článku 11 ods. 3 nariadenia (EÚ) 2022/2554 finančné subjekty zohľadňujú výsledky analýzy vplyvu na svoje činnosti (BIA). Uvedené plány reakcie a obnovy v oblasti IKT:

a) musia obsahovať podmienky, ktoré vedú k ich aktivácii alebo deaktivácii, a všetky výnimky pre takúto aktiváciu alebo deaktiváciu;

b) musia obsahovať opis toho, aké opatrenia sa majú prijať na zabezpečenie dostupnosti, integrity, kontinuity a obnovy aspoň IKT systémov a služieb podporujúcich kritické alebo dôležité funkcie finančného subjektu;

c) musia byť navrhnuté tak, aby spĺňali ciele obnovenia činností finančných subjektov;

d) musia byť zdokumentované a sprístupnené zamestnancom zapojeným do realizácie plánov reakcie a obnovy v oblasti IKT a v prípade núdze ľahko dostupné;

e) musia zabezpečovať krátkodobé aj dlhodobé možnosti obnovy vrátane čiastočného obnovenia systémov;

f) musia obsahovať ciele plánov reakcie a obnovy v oblasti IKT a podmienky vyhlásenia toho, že došlo k úspešnému vykonaniu týchto plánov.

Na účely písmena d) finančné subjekty jasne stanovia príslušné úlohy a zodpovednosti.

2. V plánoch reakcie a obnovy v oblasti IKT uvedených v odseku 1 sa určia príslušné scenáre vrátane scenárov závažných narušení činnosti a zvýšenej pravdepodobnosti výskytu narušenia. V týchto plánoch sa vypracujú scenáre na základe aktuálnych informácií o hrozbách a na základe poznatkov získaných z predchádzajúcich výskytov narušení činnosti. Finančné subjekty náležite zohľadňujú všetky tieto scenáre:

a) kybernetické útoky a prepnutia medzi primárnou infraštruktúrou IKT a redundantnou kapacitou, zálohami a redundantnými zariadeniami;

b) zhoršenie kvality poskytovania kritickej alebo dôležitej funkcie na neprijateľnú úroveň alebo jej zlyhanie, pričom sa náležite zváži potenciálny vplyv platobnej

neschopnosti alebo iných zlyhaní každého príslušného externého poskytovateľa IKT služieb;

c) čiastočné alebo úplné zlyhanie priestorov vrátane kancelárskych a obchodných priestorov a dátových centier;

d) závažné zlyhanie IKT aktív alebo komunikačnej infraštruktúry;

e) nedostupnosť kritického počtu zamestnancov alebo pracovníkov zodpovedných za zaručenie kontinuity operácií;

f) vplyv udalostí súvisiacich so zmenou klímy a zhoršovaním životného prostredia, prírodných katastrof, pandémií a fyzických útokov vrátane vniknutí a teroristických útokov;

g) útoky zvnútra subjektu;

h) politická a sociálna nestabilita, v relevantných prípadoch aj v jurisdikcii externého poskytovateľa IKT služieb, ako aj miesto, kde sa údaje uchovávajú a spracúvajú;

i) rozsiahle výpadky elektrickej energie.

3. Ak primárne opatrenia obnovy nemusia byť v krátkodobom horizonte uskutočniteľné z dôvodu nákladov, rizík, logistiky alebo neočakávaných okolností, v plánoch reakcie a obnovy v oblasti IKT uvedených v odseku 1 sa zvážia alternatívne možnosti.

4. V rámci plánov reakcie a obnovy v oblasti IKT uvedených v odseku 1 finančné subjekty zvážia a vykonajú opatrenia na zabezpečenie kontinuity s cieľom zmierniť zlyhania externých poskytovateľov IKT služieb podporujúcich kritické alebo dôležité funkcie finančného subjektu.

KAPITOLA V
SPRÁVA O PRESKÚMANÍ RÁMCA RIADENIA IKT RIZIKA

Článok 27

Formát a obsah správy o preskúmaní rámca riadenia IKT rizika

1. Finančné subjekty predkladajú správu o preskúmaní rámca riadenia IKT rizika uvedenú v článku 6 ods. 5 nariadenia (EÚ) 2022/2554 v elektronickom formáte s možnosťou vyhľadávania.

2. Finančné subjekty zahrnú do správy uvedenej v odseku 1 všetky tieto prvky:

a) úvodný oddiel, v ktorom sa:

i) jasne identifikuje finančný subjekt, ktorý je predmetom správy, a v prípade potreby opisuje jeho skupinová štruktúra;

ii) opisuje kontext správy z hľadiska povahy, rozsahu a zložitosti služieb, činností a operácií finančného subjektu, jeho organizácie, identifikovaných kritických funkcií, stratégie, hlavných prebiehajúcich projektov alebo činností, vzťahov a jeho závislosť od interných a zmluvných IKT služieb a systémov, alebo dôsledkov, ktoré by mala celková strata alebo závažná degradácia takýchto systémov z hľadiska kritických alebo dôležitých funkcií a efektívnosti trhu;

iii) sumarizujú významné zmeny v rámci riadenia IKT rizika od predloženia predchádzajúcej správy;

iv) poskytuje sumárne zhrnutie súčasného a krátkodobého profilu IKT rizika, panorámy hrozieb, posúdenia účinnosti jeho kontrol a stavu kybernetickej bezpečnosti finančného subjektu;

b) dátum schválenia správy riadiacim orgánom finančného subjektu;

c) opis dôvodu preskúmania rámca riadenia IKT rizika v súlade s článkom 6 ods. 5 nariadenia (EÚ) 2022/2554;

d) dátumy začiatku a konca obdobia preskúmania;

e) uvedenie funkcie zodpovednej za preskúmanie;

f) opis významných zmien a zlepšení rámca riadenia IKT rizika od predchádzajúceho preskúmania;

g) zhrnutie zistení preskúmania a podrobná analýza a posúdenie závažnosti slabých stránok, nedostatkov a medzier v rámci riadenia IKT rizika počas obdobia preskúmania;

h) opis opatrení na riešenie zistených slabých stránok, nedostatkov a medzier vrátane všetkých týchto prvkov:

i) zhrnutie opatrení prijatých na nápravu zistených slabých stránok, nedostatkov a medzier;

ii) očakávaný dátum vykonávania opatrení a dátumy súvisiace s vnútornou kontrolou vykonávania vrátane informácií o stave pokroku pri vykonávaní týchto opatrení k dátumu vypracovania správy, v prípade potreby s vysvetlením, či existuje riziko možného nedodržania lehôt;

iii) nástroje, ktoré sa majú použiť, a identifikácia funkcie zodpovednej za vykonávanie opatrení, pričom sa podrobne uvedie, či sú nástroje a funkcie interné alebo externé;

iv) opis vplyvu plánovaných zmien v opatreniach na rozpočtové, ľudské a materiálne zdroje finančného subjektu vrátane zdrojov určených na vykonávanie akýchkoľvek nápravných opatrení;

v) informácie o postupe informovania príslušného orgánu, ak je to vhodné;

vi) ak zistené slabé stránky, nedostatky alebo medzery nepodliehajú nápravným opatreniam, podrobné vysvetlenie kritérií použitých na analýzu vplyvu týchto slabých stránok, nedostatkov alebo medzier v snahe vyhodnotiť súvisiace zvyškové IKT riziko, ako aj kritérií použitých na akceptovanie súvisiaceho zvyškového rizika;

i) informácie o plánovanom ďalšom vývoji rámca riadenia IKT rizika;

j) závery, ktoré vyplývajú z preskúmania rámca riadenia IKT rizika;

k) informácie o predchádzajúcich preskúmaniach vrátane týchto prvkov:

i) zoznam doterajších preskúmaní;

ii) v prípade potreby stav vykonávania nápravných opatrení identifikovaných v poslednej správe;

iii) ak sa navrhované nápravné opatrenia v predchádzajúcich preskúmaniach ukázali ako neúčinné alebo priniesli neočakávané výzvy, opis spôsobu, akým by sa tieto nápravné opatrenia mohli zlepšiť, alebo opis týchto neočakávaných výziev;

l) zdroje informácií použité pri príprave správy vrátane všetkých týchto informácií:

i) v prípade finančných subjektov iných ako mikropodniky, ako sa uvádza v článku 6 ods. 6 nariadenia (EÚ) 2022/2554, výsledky vnútorných auditov;

ii) výsledky posúdení súladu;

iii) výsledky testovania digitálnej prevádzkovej odolnosti a prípadne výsledky pokročilého testovania vychádzajúceho z penetračného testovania na základe konkrétnej hrozby (TLPT), IKT nástrojov, systémov a procesov;

iv) externé zdroje.

Na účely písmena c), ak sa preskúmanie začalo v nadväznosti na pokyny orgánov dohľadu alebo na závery vyplývajúce z príslušného testovania digitálnej prevádzkovej odolnosti alebo audítorských procesov, správa musí obsahovať výslovné odkazy na takéto pokyny alebo závery, čo umožní identifikovať dôvod na začatie preskúmania. Ak sa preskúmanie začalo v nadväznosti na incidenty súvisiace s IKT, správa musí obsahovať zoznam všetkých incidentov súvisiacich s IKT a analýzu základných príčin jednotlivých incidentov.

Na účely písmena f) opis musí obsahovať analýzu vplyvu zmien na stratégiu digitálnej prevádzkovej odolnosti finančného subjektu, na rámec vnútornej kontroly IKT finančného subjektu a na správu riadenia IKT rizika finančného subjektu.

HLAVA III – ZJEDNODUŠENÝ RÁMEC RIADENIA IKT RIZIKA PRE FINANČNÉ SUBJEKTY UVEDENÝ V ČLÁNKU 16 ODS. 1 NARIADENIA (EÚ) 2022/2554

KAPITOLA I
ZJEDNODUŠENÝ RÁMEC RIADENIA IKT RIZIKA

Článok 28
Správa a riadenie a organizácia

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 musia mať zavedený rámec vnútornej správy a riadenia a kontroly, ktorým sa zabezpečuje účinné a obozretné riadenie IKT rizika s cieľom dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti.

2. Finančné subjekty uvedené v odseku 1 ako súčasť svojho zjednodušeného rámca riadenia IKT rizika zabezpečia, aby ich riadiaci orgán:

   a) niesol celkovú zodpovednosť za zabezpečenie toho, aby zjednodušený rámec riadenia IKT rizika umožňoval dosiahnutie obchodnej stratégie finančného subjektu v súlade s ochotou daného finančného subjektu podstupovať riziko, a zabezpečoval, aby sa v tejto súvislosti zohľadňovalo IKT riziko;

   b) stanovil jasné úlohy a zodpovednosti pre všetky úlohy súvisiace s IKT;

   c) stanovil ciele informačnej bezpečnosti a požiadavky na IKT;

   d) schvaľoval, dohliadal a pravidelne preskúmaval:

      i) klasifikáciu informačných aktív finančného subjektu, ako sa uvádza v článku 30 ods. 1 tohto nariadenia, zoznam identifikovaných hlavných rizík a analýzu vplyvu na podnikanie a súvisiace politiky;

      ii) plány na zabezpečenie kontinuity činností finančného subjektu a opatrenia reakcie a obnovy uvedené v článku 16 ods. 1 písm. f) nariadenia (EÚ) 2022/2554;

   e) prideľoval a preskúmaval aspoň raz ročne rozpočet potrebný na splnenie potrieb finančného subjektu v oblasti digitálnej prevádzkovej odolnosti, pokiaľ ide o všetky druhy zdrojov, vrátane relevantných programov zvyšovania informovanosti o bezpečnosti v oblasti IKT a školení o digitálnej prevádzkovej odolnosti a zručností pre všetkých zamestnancov;

   f) stanovil a vykonával politiky a opatrenia zahrnuté v kapitolách I, II a III tejto hlavy s cieľom identifikovať, posudzovať a riadiť IKT riziko, ktorému je finančný subjekt vystavený;

   g) identifikoval a vykonával postupy, IKT protokoly a nástroje, ktoré sú potrebné na ochranu všetkých informačných aktív a IKT aktív;

   h) zabezpečil, aby si zamestnanci finančného subjektu udržiavali dostatočné znalosti a zručnosti potrebné na pochopenie a posúdenie IKT rizika a jeho vplyvu na operácie finančného subjektu, ktoré zodpovedajú IKT riziku, ktoré sa má riadiť;

i) stanovil mechanizmy nahlasovania správ vrátane frekvencie, formy a obsahu nahlasovania správ riadiacemu orgánu o informačnej bezpečnosti a digitálnej prevádzkovej odolnosti.

3. Finančné subjekty uvedené v odseku 1 môžu v súlade s právom Únie a vnútroštátnym odvetvovým právom zadať úlohy overovania súladu s požiadavkami na riadenie IKT rizika vnútroskupinovým alebo externým poskytovateľom IKT služieb formou outsourcingu. V prípade takéhoto outsourcingu zostáva za overovanie súladu s požiadavkami na riadenie IKT rizika plne zodpovedný finančný subjekt.

4. Finančné subjekty uvedené v odseku 1 zabezpečia primeranú segregáciu a nezávislosť kontrolných funkcií a funkcií vnútorného auditu.

5. Finančné subjekty uvedené v odseku 1 zabezpečia, aby ich zjednodušený rámec riadenia IKT rizika podliehal vnútornému auditu vykonávanému audítormi v súlade s plánom auditu finančných subjektov. Audítori musia mať dostatočné znalosti, zručnosti a odborné znalosti v oblasti IKT rizika a musia byť nezávislí. Frekvencia a zameranie auditov IKT musia zodpovedať IKT riziku daného finančného subjektu.

6. Na základe výsledku auditu uvedeného v odseku 5 finančné subjekty uvedené v odseku 1 zabezpečia včasné overenie a nápravu kritických zistení auditu IKT.

Článok 29
Politika a opatrenia v oblasti informačnej bezpečnosti

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 vypracujú, zdokumentujú a vykonávajú politiku v oblasti informačnej bezpečnosti v kontexte zjednodušeného rámca riadenia IKT rizika. V uvedenej politike v oblasti bezpečnosti sa stanovia zásady a pravidlá na vysokej úrovni na ochranu dôvernosti, integrity, dostupnosti a pravosti údajov a služieb, ktoré tieto finančné subjekty poskytujú.

2. Finančné subjekty uvedené v odseku 1 na základe svojej politiky v oblasti informačnej bezpečnosti uvedenej v odseku 1 stanovia a vykonávajú bezpečnostné opatrenia v oblasti IKT, ktorých cieľom je zmierňovať mieru ich vystavenia IKT riziku vrátane zmierňujúcich opatrení, ktoré vykonávajú externí poskytovatelia IKT služieb.

   Bezpečnostné opatrenia v oblasti IKT zahŕňajú všetky opatrenia uvedené v článkoch 30 až 38.

Článok 30
Klasifikácia informačných aktív a IKT aktív

1. Ako súčasť zjednodušeného rámca riadenia IKT rizika uvedeného v článku 16 ods. 1 písm. a) nariadenia (EÚ) 2022/2554 finančné subjekty uvedené v odseku 1 uvedeného článku identifikujú, klasifikujú a zdokumentujú všetky kritické alebo dôležité funkcie, informačné aktíva a IKT aktíva, ktoré ich podporujú, a ich vzájomné závislosti. Finančné subjekty túto identifikáciu a klasifikáciu podľa potreby preskúmajú.

2. Finančné subjekty uvedené v odseku 1 identifikujú všetky kritické alebo dôležité funkcie podporované externými poskytovateľmi IKT služieb.

Článok 31
Riadenie IKT rizika

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 zahrnú do svojho zjednodušeného rámca riadenia IKT rizika všetky tieto prvky:

   a) určenie úrovní tolerancie rizika v prípade IKT rizika v súlade s ochotou finančného subjektu podstupovať riziko;

   b) identifikácia a posúdenie IKT rizík, ktorým je finančný subjekt vystavený;

   c) stanovenie stratégií zmierňovania aspoň pre IKT riziká, ktoré presahujú príslušné úrovne tolerancie rizika finančného subjektu;

   d) monitorovanie účinnosti stratégií zmierňovania uvedených v písmene c);

   e) identifikácia a posúdenie všetkých IKT rizík a rizík v oblasti informačnej bezpečnosti vyplývajúcich z každej významnej zmeny IKT systému alebo IKT služieb, procesov alebo postupov, ako aj z výsledkov testovania bezpečnosti IKT a po každom závažnom incidente súvisiacom s IKT.

2. Finančné subjekty uvedené v odseku 1 pravidelne vykonávajú a zdokumentujú posudzovanie IKT rizika, ktoré musí zodpovedať profilu IKT rizika finančných subjektov.

3. Finančné subjekty uvedené v odseku 1 nepretržite monitorujú hrozby a zraniteľné miesta, ktoré sú dôležité pre ich kritické alebo dôležité funkcie, informačné aktíva a IKT aktíva a pravidelne preskúmavajú rizikové scenáre, ktoré majú na tieto kritické alebo dôležité funkcie vplyv.

4. Finančné subjekty uvedené v odseku 1 stanovia varovné prahové hodnoty a kritériá na spustenie a iniciáciu procesov reakcie na incidenty súvisiace s IKT.

Článok 32
Fyzická a environmentálna bezpečnosť

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 identifikujú a vykonávajú opatrenia týkajúce sa fyzickej bezpečnosti navrhnuté na základe panorámy hrozieb a v súlade s klasifikáciou uvedenou v článku 30 ods. 1 tohto nariadenia, celkovým rizikovým profilom IKT aktív a dostupnými informačnými aktívami.

2. Opatreniami uvedenými v odseku 1 sa chránia priestory finančných subjektov a prípadne dátové centrá finančných subjektov, v ktorých sa IKT aktíva a informačné aktíva nachádzajú, pred neoprávneným prístupom, útokmi a nehodami, ako aj pred environmentálnymi hrozbami a nebezpečenstvami.

3. Ochrana pred environmentálnymi hrozbami a nebezpečenstvami zodpovedá významu dotknutých priestorov a prípadne dátových centier a kritickosti operácií alebo IKT systémov, ktoré sa v nich nachádzajú.

KAPITOLA II
ĎALŠIE PRVKY SYSTÉMOV, PROTOKOLOV A NÁSTROJOV NA MINIMALIZÁCIU VPLYVU IKT RIZIKA

Článok 33
Kontrola prístupu

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 vypracujú, zdokumentujú a vykonávajú postupy na kontrolu logického a fyzického prístupu, pričom tieto postupy presadzujú, monitorujú a pravidelne preskúmavajú. Tieto postupy obsahujú nasledujúce prvky kontroly logického a fyzického prístupu:

   a) prístupové práva k informačným aktívam, IKT aktívam a funkciám podporovaným IKT aktívami, ako aj ku kritickým miestam prevádzky finančného subjektu sa riadia na základe potreby poznať (need-to-know), zásady potreby používať (need-to-use) a zásady minimálneho privilégia (least privilege principle), a to aj v prípade vzdialeného a núdzového prístupu;

   b) zodpovednosť používateľa, ktorá zabezpečuje, aby používatelia mohli byť identifikovaní, pokiaľ ide o činnosti, ktoré v IKT systémoch vykonávajú;

   c) postupy riadenia účtov na účely udeľovania, zmeny alebo odoberania prístupových práv k používateľským a generickým účtom vrátane generických správcovských účtov;

   d) metódy autentifikácie, ktoré zodpovedajú klasifikácii uvedenej v článku 30 ods. 1 a celkovému rizikovému profilu IKT aktív a ktoré sú založené na popredných postupoch;

   e) pravidelné preskúmanie prístupových práv a ich odobratie, keď už nie sú potrebné.

   Na účely písmena c) finančný subjekt prideľuje privilegovaný, núdzový a správcovský prístup na základe potreby používať (need-to-use) alebo na *ad hoc* základe ku všetkým IKT systémom, pričom daný prístup sa zaznamená v súlade s článkom 34 ods. 1 písm. f).

   Na účely písmena d) finančné subjekty používajú silné metódy autentifikácie, ktoré sú založené na popredných postupoch v prípade vzdialeného prístupu do siete finančných subjektov, privilegovaného prístupu a prístupu k IKT aktívam podporujúcim kritické alebo dôležité funkcie, ktoré sú verejne dostupné.

Článok 34
Bezpečnosť operácií IKT

Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 ako súčasť svojich systémov, protokolov a nástrojov a v prípade všetkých IKT aktív:

a) monitorujú a riadia životný cyklus všetkých IKT aktív;

b) monitorujú, či sú IKT aktíva podporované externými poskytovateľmi IKT služieb finančných subjektov, ak je to relevantné;

c) identifikujú kapacitné požiadavky na svoje IKT aktíva a opatrenia na udržiavanie a zlepšovanie dostupnosti a efektívnosti IKT systémov a predchádzanie nedostatku IKT kapacít pred ich vznikom;

d) vykonávajú automatizované skenovanie a posudzovanie zraniteľnosti IKT aktív, ktoré zodpovedá ich klasifikácii uvedenej v článku 30 ods. 1, a celkovému rizikovému profilu IKT aktíva, a zavádzajú bezpečnostné záplaty na riešenie identifikovaných zraniteľných miest;

e) riadia riziká týkajúce sa zastaraných, nepodporovaných alebo pôvodných IKT aktív;

f) zaznamenávajú udalosti súvisiace s kontrolou logického a fyzického prístupu, operáciami IKT vrátane činností v oblasti systémovej a sieťovej prevádzky a riadením zmien IKT;

g) identifikujú a vykonávajú opatrenia s cieľom monitorovať a analyzovať informácie o anomálnych činnostiach a správaní v prípade kritických alebo dôležitých operácií IKT;

h) vykonávajú opatrenia na monitorovanie relevantných a aktuálnych informácií o kybernetických hrozbách;

i) vykonávajú opatrenia na identifikáciu možných únikov informácií, škodlivého kódu a iných bezpečnostných hrozieb a verejne známych zraniteľných miest softvéru a hardvéru, ako aj kontrolujú zodpovedajúce nové bezpečnostné aktualizácie.

Na účely písmena f) finančné subjekty zosúladia úroveň podrobnosti záznamových protokolov s ich účelom a používaním IKT aktíva, ktoré uvedené záznamové protokoly vytvára.

Článok 35
Bezpečnosť údajov, systémov a siete

Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 ako súčasť svojich systémov, protokolov a nástrojov vypracujú a zavedú záruky, ktorými sa zaistí bezpečnosť sietí pred vniknutím a zneužitím údajov, a ktorými sa zachová dostupnosť, pravosť, integrita a dôvernosť údajov. Finančné subjekty so zreteľom na klasifikáciu uvedenú v článku 30 ods. 1 tohto nariadenia stanovia najmä všetky tieto prvky:

a) identifikácia a vykonávanie opatrení na ochranu údajov pri používaní, pri prenose a v pokoji;

b) identifikácia a vykonávanie bezpečnostných opatrení týkajúcich sa používania softvéru, médií na uchovávanie údajov, systémov a koncových zariadení, ktoré prenášajú a uchovávajú údaje finančného subjektu;

c) identifikácia a vykonávanie opatrení na predchádzanie a odhaľovanie neoprávnených pripojení k sieti finančného subjektu a na zabezpečenie sieťovej prevádzky medzi internými sieťami finančného subjektu a internetom a inými externými pripojeniami;

d) identifikácia a vykonávanie opatrení, ktorými sa zabezpečí dostupnosť, pravosť, integrita a dôvernosť údajov počas prenosov v sieti;

e) postup bezpečného vymazania údajov, ktoré sa nachádzajú v priestoroch finančného subjektu alebo sú uložené externe, ktoré finančný subjekt už nemusí zhromažďovať ani uchovávať;

f) postup bezpečnej likvidácie alebo vyradenia z prevádzky pamäťových zariadení na záznam údajov, ktoré sa nachádzajú v priestoroch finančného subjektu, alebo pamäťových zariadení na záznam údajov, ktoré sú uložené externe a ktoré obsahujú dôverné informácie;

g) identifikácia a vykonávanie opatrení na zabezpečenie toho, aby telepráca a používanie súkromných koncových zariadení nemali nepriaznivý vplyv na schopnosť finančného subjektu vykonávať svoje kritické činnosti primerane, včasne a bezpečne.

Článok 36
Testovanie bezpečnosti IKT

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 vypracujú a vykonávajú plán testovania bezpečnosti IKT s cieľom overiť účinnosť svojich bezpečnostných opatrení v oblasti IKT vypracovaných v súlade s článkami 33, 34 a 35 a článkami 37 a 38 tohto nariadenia. Finančné subjekty zabezpečia, aby sa v tomto pláne zohľadnili hrozby a zraniteľné miesta identifikované ako súčasť zjednodušeného rámca riadenia IKT rizika uvedeného v článku 31 tohto nariadenia.

2. Finančné subjekty uvedené v odseku 1 preskúmajú, posúdia a testujú bezpečnostné opatrenia v oblasti IKT, pričom zohľadnia celkový rizikový profil IKT aktív finančného subjektu.

3. Finančné subjekty uvedené v odseku 1 monitorujú a vyhodnocujú výsledky bezpečnostných testov, pričom v prípade IKT systémov podporujúcich kritické alebo dôležité funkcie bez zbytočného odkladu príslušným spôsobom aktualizujú svoje bezpečnostné opatrenia.

Článok 37
Nadobudnutie, vývoj a údržba IKT systémov

Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 v prípade potreby navrhnú a vykonávajú postup, ktorým sa riadi nadobudnutie, vývoj a údržba IKT systémov na základe prístupu založeného na riziku. Týmto postupom sa:

a) zabezpečí, aby pred každým nadobudnutím alebo vývojom IKT systémov dotknutá obchodná funkcia jasne špecifikovala a schválila funkčné a nefunkčné požiadavky vrátane požiadaviek na bezpečnosť informácií;

b) zabezpečí testovanie a schvaľovanie IKT systémov pred ich prvým použitím a pred zavedením zmien do ich produkčného prostredia;

c) identifikujú opatrenia na zmiernenie rizika neúmyselnej zmeny IKT systémov alebo úmyselnej manipulácie s IKT systémami počas ich vývoja a vykonávania v produkčnom prostredí.

Článok 38
Riadenie IKT projektu a zmien

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 vypracujú, zdokumentujú a vykonávajú postup riadenia IKT projektu a stanovia úlohy a zodpovednosti pre jeho vykonávanie. Tento postup sa vzťahuje na všetky fázy IKT projektov od ich začatia až po ich ukončenie.

2. Finančné subjekty uvedené v odseku 1 vypracujú, zdokumentujú a vykonávajú postup riadenia IKT zmien s cieľom zabezpečiť, aby sa všetky zmeny IKT systémov zaznamenávali, testovali, posudzovali, schválili, vykonávali a overovali kontrolovane a s primeranými zárukami na zachovanie digitálnej prevádzkovej odolnosti finančného subjektu.

Kapitola III
RIADENIE KONTINUITY ČINNOSTÍ V OBLASTI IKT

Článok 39
Zložky plánu kontinuity činností v oblasti IKT

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 vypracujú svoje plány kontinuity činností v oblasti IKT, pričom zohľadnia výsledky analýzy svojich expozícií a potenciálneho vplyvu závažných narušení činnosti a scenárov, ktorým by mohli byť vystavené ich IKT aktíva podporujúce kritické alebo dôležité funkcie, vrátane scenára kybernetického útoku.

2. Plány kontinuity činnosti v oblasti IKT uvedené v odseku 1 musia:

   a) byť schválené riadiacim orgánom finančného subjektu;

   b) byť zdokumentované a ľahko prístupné v prípade núdzovej alebo krízovej situácie;

   c) mať vyčlenené dostatočné zdroje na svoje vykonávanie;

   d) stanoviť plánované úrovne obnovy a časové rámce na obnovu a obnovenie funkcií a kľúčových interných a externých závislostí vrátane externých poskytovateľov IKT služieb;

   e) identifikovať podmienky, ktoré môžu viesť k aktivácii plánov kontinuity činností v oblasti IKT, a opatrenia, ktoré sa majú prijať na zabezpečenie dostupnosti, kontinuity a obnovy IKT aktív finančných subjektov podporujúcich kritické alebo dôležité funkcie;

   f) identifikovať opatrenia na reštaurovanie a obnovu kritických alebo dôležitých obchodných funkcií, podporných procesov, informačných aktív a ich vzájomných závislostí s cieľom zabrániť nepriaznivým účinkom na fungovanie finančných subjektov;

   g) identifikovať postupy a opatrenia zálohovania, v ktorých sa bližšie určí rozsah údajov, ktoré sú predmetom zálohovania, a minimálna frekvencia zálohovania na základe kritickosti informácií používajúcich uvedené údaje;

   h) zvážiť alternatívne možnosti, ak by obnova nebola možná z krátkodobého hľadiska z dôvodu nákladov, rizík, logistiky alebo neočakávaných okolností;

   i) stanoviť mechanizmy internej a externej komunikácie vrátane plánov eskalácie;

   j) byť aktualizované v súlade s poznatkami získanými z incidentov, testov, nových rizík a identifikovaných hrozieb, zmenených cieľov obnovy, významných zmien v organizácii finančného subjektu a IKT aktív podporujúcich kritické alebo obchodné funkcie.

   Na účely písmena f) sa opatreniami uvedenými v uvedenom písmene stanoví zmierňovanie zlyhaní kritických poskytovateľov, ktorí sú tretími stranami.

Článok 40
Testovanie plánov kontinuity činností

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 testujú svoje plány kontinuity činností uvedené v článku 39 tohto nariadenia vrátane scenárov uvedených v danom článku, a to aspoň raz ročne na účely postupov zálohovania a obnovenia činnosti alebo pri každej významnej zmene plánu kontinuity činností.

2. Testovaním plánov kontinuity činností uvedených v odseku 1 sa preukazuje, že finančné subjekty uvedené v danom odseku dokážu udržiavať životaschopnosť svojich činností až do obnovenia kritických operácií a identifikovať všetky nedostatky v uvedených plánoch.

3. Finančné subjekty uvedené v odseku 1 zdokumentujú výsledky testovania plánov kontinuity činností, pričom všetky zistené nedostatky vyplývajúce z tohto testovania sa musia analyzovať, riešiť a nahlásiť riadiacemu orgánu.

KAPITOLA IV
SPRÁVA O PRESKÚMANÍ ZJEDNODUŠENÉHO RÁMCA RIADENIA IKT RIZIKA

Článok 41
Formát a obsah správy o preskúmaní zjednodušeného rámca riadenia IKT rizika

1. Finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554 predložia správu o preskúmaní rámca riadenia IKT rizika uvedenú v odseku 2 tohto článku v elektronickom formáte s možnosťou vyhľadávania.

2. Správa uvedená v odseku 1 obsahuje všetky tieto informácie:

   a) úvodný oddiel, ktorý obsahuje tieto časti:

      i) opis kontextu správy z hľadiska povahy, rozsahu a zložitosti služieb finančného subjektu, jeho činností a operácií, organizácie finančného subjektu, identifikovaných kritických funkcií, stratégie, hlavných prebiehajúcich projektov alebo činností a vzťahov, ako aj z hľadiska závislosti finančného subjektu od interných IKT služieb a systémov a služieb a systémov zabezpečovaných na základe outsourcingu, alebo dôsledkov, ktoré by mala celková strata alebo závažná degradácia takýchto systémov na kritické alebo dôležité funkcie a efektívnosť trhu;

      ii) sumárne zhrnutie súčasného a krátkodobého profilu identifikovaného IKT rizika, panorámy hrozieb, posúdenia účinnosti jeho kontrol a stavu kybernetickej bezpečnosti finančného subjektu;

      iii) informácie o nahlasovanej časti uvedenej správy;

      iv) zhrnutie významných zmien v rámci riadenia IKT rizika od predloženia predchádzajúcej správy;

      v) zhrnutie a opis vplyvu významných zmien na zjednodušený rámec riadenia IKT rizika od predloženia predchádzajúcej správy;

   b) prípadne dátum schválenia správy riadiacim orgánom finančného subjektu;

   c) opis dôvodov preskúmania vrátane týchto informácií:

i) ak sa preskúmanie začalo v nadväznosti na pokyny orgánu dohľadu, dôkaz o takýchto pokynoch;

ii) ak sa preskúmanie začalo v nadväznosti na incidenty súvisiace s IKT, zoznam všetkých uvedených incidentov súvisiacich s IKT spolu so súvisiacou analýzou základných príčin incidentov;

d) dátumy začiatku a konca obdobia preskúmania;

e) osoba zodpovedná za preskúmanie;

f) zhrnutie zistení a vlastné hodnotenie závažnosti slabých miest, nedostatkov a medzier zistených v rámci riadenia IKT rizika počas obdobia preskúmania vrátane ich podrobnej analýzy;

g) nápravné opatrenia identifikované na riešenie slabých miest, nedostatkov a medzier v zjednodušenom rámci riadenia IKT rizika, ako aj očakávaný dátum vykonávania uvedených opatrení vrátane následných opatrení týkajúcich sa slabých stránok, nedostatkov a medzier identifikovaných v predchádzajúcich správach, ak tieto slabé miesta, nedostatky a medzery ešte neboli odstránené;

h) celkové závery o preskúmaní zjednodušeného rámca riadenia IKT rizika vrátane každého ďalšieho plánovaného vývoja.

HLAVA IV – ZÁVEREČNÉ USTANOVENIA

Článok 42
Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 13. 3. 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN