2

VYHLÁŠKA

ze dne 22. prosince 2021,

kterou se mění vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu

Česká národní banka stanoví podle § 263 zákona č. 370/2017 Sb., o platebním styku, k provedení § 16 odst. 5, § 17 odst. 3, § 20 odst. 4, § 46 odst. 2, § 48 odst. 4, § 59 odst. 4, § 65a odst. 2, § 74 odst. 6, § 75 odst. 3, § 78 odst. 4 a § 100 odst. 4 tohoto zákona:

Čl. I

Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu, se mění takto:

1. § 1 včetně nadpisu a poznámky pod čarou č. 1 zní:

„§ 1

Předmět úpravy

Tato vyhláška zapracovává příslušné předpisy Evropské unie[1]) a upravuje

a) způsob plnění některých požadavků na řídicí a kontrolní systém platební instituce, instituce elektronických peněz a správce informací o platebním účtu,

b) způsob plnění požadavků na systém řízení bezpečnostních a provozních rizik a systém vyřizování stížností a reklamací u poskytovatele platebních služeb malého rozsahu a vydavatele elektronických peněz malého rozsahu,

c) pravidla pro výpočet výše kapitálu a kapitálové přiměřenosti platební instituce a instituce elektronických peněz včetně jednotlivých přístupů, které se mohou při výpočtu kapitálové přiměřenosti uplatňovat,

d) minimální limit pojistného plnění z pojištění a minimální výši srovnatelného zajištění pro platební instituci, instituci elektronických peněz a správce informací o platebním účtu.

[1]) Čl. 4 bod 46, čl. 8 odst. 2, čl. 9, čl. 9 odst. 1 /část/ a čl. 9 odst. 2 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES.
Čl. 5 odst. 2, čl. 5 odst. 3, čl. 5 odst. 4 a čl. 5 odst. 6 směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, o změně směrnic 2005/60/ES a 2006/48/ES a o zrušení směrnice 2000/46/ES.“.

2. Část druhá včetně nadpisu zní:

„ČÁST DRUHÁ

ZPŮSOB PLNĚNÍ NĚKTERÝCH POŽADAVKŮ

HLAVA I

ZPŮSOB PLNĚNÍ NĚKTERÝCH POŽADAVKŮ NA ŘÍDICÍ A KONTROLNÍ SYSTÉM PLATEBNÍ INSTITUCE

(K § 20 odst. 4 zákona)

§ 2

Vnitřní předpisy

(1) Platební instituce zapracuje požadavky stanovené na řídicí a kontrolní systém a postupy k jejich naplňování do svých vnitřních předpisů, kterými se rozumí strategie, organizační řád, plány a další vnitřně stanovené zásady a postupy platební instituce.

(2) Platební instituce stanoví a uplatňuje postup pro přijímání a změny vnitřních předpisů a zajistí, aby vnitřní předpisy byly pravidelně vyhodnocovány a případně upravovány.

(3) Platební instituce zajistí, aby vnitřní předpisy byly v souladu s údaji uvedenými v žádosti

o udělení povolení k činnosti platební instituce nebo jejích přílohách, na jejichž základě bylo povolení k činnosti uděleno, případně změněnými podle § 11 zákona.

(4) Platební instituce zohlední ve vnitřních předpisech obecné pokyny a doporučení vydané Evropským orgánem pro bankovnictví, Evropským orgánem pro cenné papíry a trhy, Evropským orgánem pro pojišťovnictví a zaměstnanecké penzijní pojištění nebo Společným výborem evropských orgánů dohledu a určené poskytovatelům platebních služeb.

(5) Platební instituce zajistí, aby všichni pracovníci byli s příslušnými vnitřními předpisy a jejich případnými změnami v potřebném rozsahu seznámeni a postupovali v souladu s nimi.

§ 3

Schvalovací a rozhodovací procesy

Platební instituce zajistí, aby byla srozumitelně stanovena oprávnění ke schvalování a podepisování dokumentů v rámci činnosti platební instituce a aby veškeré relevantní schvalovací a rozhodovací procesy a kontrolní činnosti včetně souvisejících působností a pravomocí v rámci činnosti platební instituce a jejích vnitřních předpisů bylo možné zaznamenávat, uchovávat a zpětně vysledovat a rekonstruovat. Za tímto účelem vhodně upraví také své informační a komunikační systémy.

§ 4

Systém řízení bezpečnostních a provozních rizik

(1) Platební instituce zavede k řízení bezpečnostních a provozních rizik souvisejících s platebními službami, které poskytuje, opatření pro zmírnění těchto rizik a kontrolní mechanismy. Platební instituce stanoví a udržuje účinné postupy řízení bezpečnostních a provozních incidentů, a to i pro odhalování a klasifikaci závažných bezpečnostních a provozních incidentů.

(2) Platební instituce v rámci systému řízení bezpečnostních a provozních rizik řídí vždy také rizika v oblasti informačních a komunikačních technologií a bezpečnosti, která zahrnují alespoň

a) rizika ztráty v důsledku narušení důvěrnosti dat, integrity systémů a dat nebo dostupnosti systémů a dat nebo v důsledku neschopnosti změnit informační a komunikační systémy v přiměřeném čase a s přiměřenými náklady, pokud se mění prostředí nebo činnosti,
b) bezpečnostní rizika vyplývající z nedostatečnosti nebo selhání vnitřních procesů nebo z vnějších událostí včetně kybernetických útoků nebo z nedostatečného fyzického zabezpečení.

(3) Podrobnosti k řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti, kterým platební instituce je nebo by mohla být vystavena v souvislosti s jí poskytovanými platebními službami, jsou uvedeny v příloze k této vyhlášce.

(4) Platební instituce vypracuje politiku bezpečnosti informací, která vymezuje zásady a pravidla na ochranu důvěrnosti, integrity a dostupnosti dat a informací platební instituce a uživatelů platebních služeb. Platební instituce upraví ve svých vnitřních předpisech bezpečnostní opatření v souladu s podrobnostmi k řízení rizik podle přílohy k této vyhlášce.

§ 5

Systém vyřizování stížností a reklamací

(1) Platební instituce zavede a uplatňuje postupy pro nakládání se stížnostmi a reklamacemi uživatelů platebních služeb, které

a) jsou schváleny osobou, která skutečně řídí činnost platební instituce v oblasti poskytování platebních služeb, přičemž tato osoba také průběžně kontroluje jejich dodržování,
b) jsou stanoveny ve vnitřním předpisu,
c) umožňují jejich řádné prošetřování a zajišťují identifikaci a zmírňování možných střetů zájmů při nakládání s nimi.

(2) Platební instituce interně eviduje v souladu se stanovenými lhůtami stížnosti a reklamace a nakládání s nimi, a to způsobem splňujícím požadavky na bezpečnost informací.

(3) Platební instituce nastaví systém pro vyřizování stížností a reklamací tak, že jí umožňuje poskytovat bez zbytečného odkladu České národní bance na vyžádání informace o stížnostech a reklamacích a o nakládání s nimi včetně konkrétních postupů jejich vyřizování.

(4) Platební instituce průběžně analyzuje údaje o stížnostech a reklamacích a výsledcích jejich vyřízení s cílem zabezpečit identifikaci a řešení pří-

padných systémových nedostatků a možných rizik, alespoň

a) analyzuje důvody jednotlivých stížností a reklamací a identifikuje hlavní příčiny jednotlivých druhů stížností a reklamací,
b) posuzuje, zda identifikované hlavní příčiny mohou ovlivnit i jiné procesy, služby nebo produkty, včetně těch, kterých se stížnost nebo reklamace přímo netýká,
c) v případě systémových nedostatků vždy provádí odstranění identifikovaných příčin stížností a reklamací.

(5) Platební instituce

a) poskytne uživateli platebních služeb na požádání a vždy v souvislosti s potvrzením přijetí stížnosti nebo reklamace písemnou informaci o svém postupu vyřizování stížnosti nebo reklamace, a to v českém jazyce nebo v jiném jazyce, pokud se na něm s uživatelem platebních služeb dohodla,
b) zpřístupní uživatelům platebních služeb a veřejnosti informace podle písmene c) prostřednictvím adres elektronické pošty uživatelů platebních služeb nebo jiným způsobem dohodnutým s uživateli platebních služeb ve svých obchodních prostorách, a má-li zřízeny internetové stránky, také na nich, a to alespoň v českém jazyce,
c) poskytuje srozumitelné, přesné a aktuální informace o postupu vyřizování stížností a reklamací, které zahrnují
   1. podrobné údaje o tom, jak stížnost nebo reklamaci podat, zejména druh informací, které musí uživatel platebních služeb uvést, a kontaktní údaje osoby nebo útvaru platební instituce, kterým má být stížnost nebo reklamace zaslána,
   2. informace o lhůtě, ve které bude uživatel platebních služeb vyrozuměn o vyřízení stížnosti, a o orientační lhůtě zpracování stížnosti nebo reklamace,
   3. podstatné průběžné informace o zpracovávání stížnosti nebo reklamace,
   4. informace o kontaktních údajích České národní banky, Kanceláře finančního arbitra a Kanceláře veřejného ochránce práv.

(6) Platební instituce

a) vyvine úsilí, které lze po ní rozumně požadovat, aby získala a prověřila všechny relevantní důkazy a informace týkající se dané stížnosti nebo reklamace,
b) komunikuje s uživatelem platebních služeb jednoduchým a srozumitelným způsobem,
c) poskytuje odpovědi bez zbytečného odkladu a nejpozději ve lhůtách podle § 258 zákona; nemůže-li tyto lhůty dodržet, informuje uživatele platebních služeb o důvodech prodlení a termínu, kdy bude vyřízení stížnosti nebo reklamace dokončeno,
d) při zaujetí stanoviska, které plně nevyhovuje požadavkům uživatele platebních služeb, v něm podrobně vysvětlí řešení stížnosti nebo reklamace a uvede informaci o možnosti uživatele platebních služeb na stížnosti nebo reklamaci trvat a obrátit se na Kancelář finančního arbitra, Českou národní banku a ve věcech práva na rovné zacházení a ochrany před diskriminací na Kancelář veřejného ochránce práv, přičemž součástí jsou kontaktní údaje daného orgánu, nebo na soud.

HLAVA II

ZPŮSOB PLNĚNÍ NĚKTERÝCH POŽADAVKŮ NA ŘÍDICÍ A KONTROLNÍ SYSTÉM INSTITUCE ELEKTRONICKÝCH PENĚZ

(K § 78 odst. 4 zákona)

§ 6

Pro instituci elektronických peněz se použijí § 2 až 5 obdobně.

HLAVA III

ZPŮSOB PLNĚNÍ NĚKTERÝCH POŽADAVKŮ NA ŘÍDICÍ A KONTROLNÍ SYSTÉM SPRÁVCE INFORMACÍ O PLATEBNÍM ÚČTU

(K § 48 odst. 4 zákona)

§ 7

(1) Pro správce informací o platebním účtu se použijí § 2 a 3 obdobně.

(2) Pro naplňování požadavků na systém řízení bezpečnostních a provozních rizik postupuje správce informací o platebním účtu obdobně podle § 4.

(3) Pro naplňování požadavků na vyřizování stížností a reklamací postupuje správce informací o platebním účtu obdobně podle § 5.

HLAVA IV

ZPŮSOB PLNĚNÍ POŽADAVKŮ NA SYSTÉM ŘÍZENÍ BEZPEČNOSTNÍCH A PROVOZNÍCH RIZIK A SYSTÉM VYŘIZOVÁNÍ STÍŽNOSTÍ A REKLAMACÍ U POSKYTOVATELE PLATEBNÍCH SLUŽEB MALÉHO ROZSAHU

(K § 59 odst. 4 zákona)

§ 8

(1) Poskytovatel platebních služeb malého rozsahu promítne požadavky stanovené na systém řízení bezpečnostních a provozních rizik a systém vyřizování stížností a reklamací do svých vnitřních předpisů a pro naplňování požadavků na tyto vnitřní předpisy postupuje obdobně podle § 2 odst. 2 až 5.

(2) Pro naplňování požadavků na schvalovací a rozhodovací procesy týkající se systému řízení bezpečnostních a provozních rizik a systému vyřizování stížností a reklamací postupuje poskytovatel platebních služeb malého rozsahu obdobně podle § 3.

(3) Pro naplňování požadavků na systém řízení bezpečnostních a provozních rizik souvisejících s poskytováním platebních služeb postupuje poskytovatel platebních služeb malého rozsahu obdobně podle § 4.

(4) Pro naplňování požadavků na systém vyřizování stížností a reklamací postupuje poskytovatel platebních služeb malého rozsahu obdobně podle § 5.

HLAVA V

ZPŮSOB PLNĚNÍ POŽADAVKŮ NA SYSTÉM ŘÍZENÍ BEZPEČNOSTNÍCH A PROVOZNÍCH RIZIK A SYSTÉM VYŘIZOVÁNÍ STÍŽNOSTÍ A REKLAMACÍ U VYDAVATELE ELEKTRONICKÝCH PENĚZ MALÉHO ROZSAHU

(K § 100 odst. 4 zákona)

§ 9

(1) Vydavatel elektronických peněz malého rozsahu promítne požadavky stanovené na systém řízení bezpečnostních a provozních rizik a systém vyřizování stížností a reklamací do svých vnitřních předpisů a pro naplňování požadavků na tyto vnitřní předpisy postupuje obdobně podle § 2 odst. 2 až 5.

(2) Pro naplňování požadavků na schvalovací a rozhodovací procesy týkající se systému řízení bezpečnostních a provozních rizik a systému vyřizování stížností a reklamací postupuje vydavatel elektronických peněz malého rozsahu obdobně podle § 3.

(3) Pro naplňování požadavků na systém řízení bezpečnostních a provozních rizik postupuje vydavatel elektronických peněz malého rozsahu obdobně podle § 4.

(4) Pro naplňování požadavků na systém vyřizování stížností a reklamací postupuje vydavatel elektronických peněz malého rozsahu obdobně podle § 5.“.

Poznámky pod čarou č. 2 až 4 se zrušují.

3. V § 27 odstavec 4 zní:

„(4) Platební instituce, která vykonává i jiné podnikatelské činnosti než činnost, k jejímuž výkonu je oprávněna na základě povolení uděleného podle zákona, (dále jen „hybridní platební instituce“) nesmí do kapitálu určeného podle odstavce 1 zahrnout ty položky nebo jejich části, které jsou použity pro výkon jiných činností, než jsou činnosti, k jejichž výkonu je oprávněna na základě povolení uděleného podle zákona.“.

4. V § 34 se vkládá nový odstavec 1, který zní:

„(1) Kapitál se vypočítá obdobně jako kapitál podle čl. 4 odst. 1 bodu 118 nařízení.“.

Dosavadní odstavce 1 až 5 se označují jako odstavce 2 až 6.

5. V § 34 odstavec 4 zní:

„(4) Instituce elektronických peněz, která vykonává i jiné podnikatelské činnosti než činnost, k jejímuž výkonu je oprávněna na základě povolení uděleného podle zákona, nesmí do kapitálu určeného podle odstavce 1 zahrnout ty položky nebo jejich části, které jsou použity pro výkon jiných činností, než jsou činnosti, k jejichž výkonu je oprávněna na základě povolení uděleného podle zákona.“.

6. Doplňuje se příloha, která zní:

„Příloha k vyhlášce č. 7/2018 Sb.

Podrobnosti k řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti

Přiměřenost

1. Platební instituce dodržuje požadavky na řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti (dále jen „rizika IKT a bezpečnosti“) způsobem, který je přiměřený velikosti platební instituce, jejímu organizačnímu uspořádání a povaze, rozsahu, složitosti a rizikovosti služeb a produktů, které platební instituce poskytuje nebo zamýšlí poskytovat.

Strategické a operativní řízení, organizační uspořádání

2. Osoba, která skutečně řídí činnost platební instituce v oblasti poskytování platebních služeb (dále jen „vedoucí pracovník“) zajistí, aby platební instituce měla zaveden adekvátní rámec vnitřní správy a řízení a vnitřní kontroly pro rizika IKT a bezpečnosti. Vedoucí pracovník srozumitelně vymezí role a povinnosti pro funkce v oblasti informačních a komunikačních technologií, řízení rizik IKT a bezpečnosti včetně bezpečnosti informací a plynulého výkonu činností a trvalého fungování platební instituce, a to i pro sebe.
3. Vedoucí pracovník zajistí, aby počet pracovníků platební instituce a jejich odborná způsobilost a zkušenosti byly přiměřené pro průběžnou podporu provozu platební instituce v oblasti informačních a komunikačních technologií, řízení rizik IKT a bezpečnosti a pro zajištění realizace její strategie v oblasti informačních a komunikačních technologií a aby tomu odpovídal přidělený rozpočet. Platební instituce zajistí, aby všichni pracovníci alespoň jednou ročně absolvovali vhodné školení odborné přípravy se zaměřením na rizika IKT a bezpečnosti, včetně bezpečnosti informací (bod 49).
4. V působnosti vedoucího pracovníka je stanovení a schvalování strategie platební instituce v oblasti informačních a komunikačních technologií v rámci celkové strategie platební instituce, dohled nad implementací této strategie a vytvoření účinného rámce řízení rizik IKT a bezpečnosti.

5. Strategie v oblasti informačních a komunikačních technologií je v souladu s celkovou strategií platební instituce a vymezuje

   a) jak by se měly informační a komunikační technologie platební instituce rozvíjet, aby účinně podporovaly celkovou strategii platební instituce, včetně vymezení vývoje organizačního uspořádání, změn v systémech informačních a komunikačních technologií (dále jen „IKT systémy“) a klíčových vztahů závislosti na třetích stranách,

   b) plánovanou strategii a vývoj architektury informačních a komunikačních technologií, včetně vztahů závislosti na třetích stranách,

   c) srozumitelné cíle v oblasti bezpečnosti informací se zaměřením na IKT systémy a služby, pracovníky a procesy v oblasti informačních a komunikačních technologií.

6. Platební instituce stanoví soubory akčních plánů, které obsahují opatření nutná k naplnění strategie v oblasti informačních a komunikačních technologií. S těmito plány jsou seznámeni všichni příslušní pracovníci a další příslušné osoby včetně dodavatelů a externích poskytovatelů služeb nebo činností, kterými se rozumí poskytovatelé outsourcingu, poskytovatelé v rámci skupiny, jejímž je platební instituce členem, nebo jiní externí poskytovatelé (dále jen „externí poskytovatelé“), pokud jsou pro ně použitelné a významné. Platební instituce akční plány pravidelně přezkoumává a zajišťuje jejich soustavnou relevanci a vhodnost. Platební instituce zavede procesy ke sledování a vyhodnocování účinnosti provádění její strategie v oblasti informačních a komunikačních technologií.

7. Platební instituce zajistí, že opatření ke zmírnění rizik vymezená v rámci systému řízení rizik jsou účinná i v případě, že jakékoli provozní funkce poskytování platebních služeb nebo IKT systémy či služby v oblasti informačních a komunikačních technologií (dále jen „IKT služby“) jsou zajišťovány externě.

8. Pro plynulé využívání IKT systémů a IKT služeb platební instituce zajistí, že smlouvy a obdobná ujednání o úrovni služeb se všemi externími poskytovateli zahrnují

   a) cíle a opatření související s bezpečností informací včetně konkrétních požadavků a kritérií; v tom vždy minimální požadavky na kybernetickou bezpečnost, specifikace životního cyklu dat platební instituce, veškeré požadavky týkající se šifrování dat, procesů zabezpečení sítě a sledování bezpečnosti a umístění datových center,

   b) provozní postupy a postupy pro řešení jednorázových událostí nebo řady souvisejících událostí neplánovaných platební institucí, která má nebo pravděpodobně bude mít nepříznivý dopad na integritu, dostupnost, důvěrnost nebo autenticitu služeb (dále jen „bezpečnostní a provozní incident“), včetně předávání na vyšší úroveň řízení a podávání zpráv.

9. Platební instituce sleduje a ujišťuje se, že externí poskytovatelé zajišťují požadovanou úroveň bezpečnostních cílů, opatření a provozních úkolů platební instituce, které externě zajišťují.

Systém řízení rizik IKT a bezpečnosti

10. Platební instituce rozpoznává a řídí rizika IKT a bezpečnosti, kterým je nebo by mohla být vystavena v souvislosti s jí poskytovanými platebními službami. Uplatňuje při tom postupy a kontroly, které zajišťují, že všechna tato rizika budou

rozpoznávána, vyhodnocována, měřena, sledována, ohlašována a omezována v souladu se schválenou mírou ochoty platební instituce přistupovat k těmto rizikům, a realizované projekty a systémy a prováděné činnosti jsou v souladu s dalšími vnitřně stanovenými pravidly platební instituce a požadavky stanovenými právními předpisy nebo opatřeními k nápravě uloženými Českou národní bankou.

11. Platební instituce svěří působnost za řízení rizik IKT a bezpečnosti a za dohled nad těmito riziky kontrolní funkci. Platební instituce zajistí nezávislost a objektivitu této kontrolní funkce tak, že ji vhodným způsobem oddělí od provozní činnosti v oblasti informačních a komunikačních technologií. Tato kontrolní funkce je přímo odpovědná vedoucímu pracovníkovi a v její působnosti je sledování a kontrola systému řízení rizik IKT a bezpečnosti. Zajišťuje rovněž, aby rizika IKT a bezpečnosti byla rozpoznávána, vyhodnocována, měřena, sledována a ohlašována. Platební instituce zajistí, aby tato kontrolní funkce neměla v působnosti žádný vnitřní audit.

12. K zajištění účinného systému řízení rizik IKT a bezpečnosti platební instituce vymezí klíčové role a povinnosti, příslušné hierarchické vztahy a s nimi související působnosti. Platební instituce zajistí, že řízení rizik IKT a bezpečnosti je plně integrováno do systému řízení rizik platební instituce, včetně zajištění efektivnosti a bezrozpornosti vazeb v rámci tohoto systému a je v souladu s jednotlivými procesy systému řízení rizik.

13. Systém řízení rizik IKT a bezpečnosti zahrnuje procesy pro

    a) určení míry ochoty platební instituce přistupovat k těmto rizikům v souladu s mírou ochoty platební instituce přistupovat k rizikům,

    b) rozpoznávání a vyhodnocování těchto rizik, kterým je platební instituce vystavena,

    c) přijímání opatření vedoucích k omezení výskytu nebo dopadu výskytu těchto rizik,

    d) sledování účinnosti opatření a počtu oznámených bezpečnostních a provozních incidentů v oblasti platebního styku, včetně incidentů podle § 221 zákona, které mají dopad na činnosti související s informačními a komunikačními technologiemi, a v případě potřeby přijímání opatření,

    e) ohlašování těchto rizik a opatření vedoucímu pracovníkovi,

    f) rozpoznání a vyhodnocování těchto rizik vyplývajících z jakékoli významné změny v IKT systémech a IKT službách, procesech či postupech nebo v návaznosti na jakýkoli významný bezpečnostní a provozní incident.

14. Platební instituce zajistí, aby systém řízení rizik IKT a bezpečnosti byl řádně zdokumentován a soustavně zdokonalován na základě získaných poznatků. Vedoucí pracovník alespoň jednou ročně schvaluje a přezkoumává nastavení systému řízení rizik IKT a bezpečnosti.

15. Platební instituce identifikuje a mapuje obchodní funkce, role a podpůrné procesy z hlediska jejich významu a vzájemných vazeb v souvislosti s riziky IKT a bezpečnosti.

16. Platební instituce také identifikuje shromážděné informace, které je třeba chránit (dále jen „informační aktivum“), podporující obchodní funkce a podpůrné procesy a zavede a aktualizuje jejich monitorování. Platební instituce je schopna řídit vždy informační aktiva, která podporují její kritické obchodní funkce a procesy.

17. Platební instituce klasifikuje identifikované obchodní funkce, podpůrné procesy a informační aktiva podle bodů 15 a 16 z hlediska jejich kritičnosti.

18. Za účelem definování kritičnosti těchto identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv platební instituce zvažuje alespoň požadavky týkající se důvěrnosti, integrity a dostupnosti. Platební instituce srozumitelně vymezí povinnosti a odpovědnosti týkající se informačních aktiv.

19. Platební instituce přezkoumává přiměřenost klasifikace informačních aktiv a příslušné dokumentace vždy, když provádí vyhodnocení rizik.

20. Platební instituce rozpoznává rizika IKT a bezpečnosti, která mají dopad na identifikované a klasifikované obchodní funkce, podpůrné procesy a informační aktiva, a to podle jejich kritičnosti. Toto vyhodnocování rizik provádí, včetně zdokumentování, alespoň jednou ročně a vždy při všech velkých změnách infrastruktury, procesů nebo postupů ovlivňujících obchodní funkce, podpůrné procesy nebo informačních aktiva. Na základě toho platební instituce aktualizuje platné vyhodnocení rizik.

21. Platební instituce průběžně sleduje hrozby a zranitelnost významné pro obchodní funkce, podpůrné procesy a informační aktiva a pravidelně přezkoumává scénáře rizik, které na ně mají dopad.

22. Na základě vyhodnocení rizik platební instituce určí opatření vedoucí k omezení rozpoznaných rizik IKT a bezpečnosti na úroveň odpovídající míře ochoty platební instituce přistupovat k rizikům. Platební instituce také určí, zda jsou potřebné změny stávajících obchodních procesů, kontrolních opatření, IKT systémů a IKT služeb. Platební instituce zváží čas potřebný k provedení těchto změn a čas na přijetí příslušných prozatímních opatření vedoucích k omezení rizik IKT a bezpečnosti v míře ochoty platební instituce k těmto rizikům přistupovat.

23. Platební instituce přijímá opatření vedoucí k omezení rozpoznaných rizik IKT a bezpečnosti a k ochraně informačních aktiv v souladu s jejich klasifikací.

24. Platební instituce zajistí, že výsledky vyhodnocování rizik jsou srozumitelně a včas oznamovány vedoucímu pracovníkovi.

Vnitřní audit v oblasti rizik IKT a bezpečnosti

25. Funkce vnitřního auditu uplatňuje rizikově orientovaný přístup a samostatně přezkoumává soulad všech činností platební instituce souvisejících s informačními a komunikačními technologiemi a bezpečností se zásadami a postupy platební instituce a s externími požadavky, přezkoumává, zda tyto zásady a postupy jsou v dotčených útvarech dodržovány, a poskytuje o tom objektivní nezávislé ujištění. Funkce vnitřního auditu, kterou platební instituce zajišťuje interně nebo externě, pravidelně poskytuje vedoucímu pracovníkovi nezávislé ujištění o účinnosti systému řízení rizik IKT a bezpečnosti. Pracovníci, kteří zajišťují funkci vnitřního auditu, jsou odborně způsobilí a mají dostatečné zkušenosti týkající se rizik IKT a bezpečnosti, plateb a jsou v rámci platební instituce nebo na dotčené platební instituci nezávislí. Četnost a zaměření auditů odpovídá závažnosti těchto rizik.

26. Vedoucí pracovník schvaluje plán auditů, včetně všech auditů v oblasti informačních a komunikačních technologií a jakýchkoli jejich podstatných změn. Plán auditů a jeho provádění, včetně četnosti auditů, odráží inherentní rizika IKT a bezpečnosti platební instituce, je úměrný těmto rizikům a je pravidelně aktualizován.

27. Platební instituce stanoví opatření pro včasné ověření a nápravu kritických zjištění auditů v oblasti informačních a komunikačních technologií.

Bezpečnost informací

Politika bezpečnosti informací

28. Platební instituce zajistí, že politika bezpečnosti informací je v souladu s cíli platební instituce v oblasti bezpečnosti informací a je založena na výsledcích vyhodnocování rizik. Politiku bezpečnosti informací schvaluje vedoucí pracovník.

29. Politika bezpečnosti zahrnuje popis hlavních rolí a povinností v oblasti řízení bezpečnosti informací a požadavky na pracovníky a externí poskytovatele, procesy a technologie v souvislosti s bezpečností informací. Všichni pracovníci a externí poskytovatelé mají povinnosti při zajišťování bezpečnosti informací platební instituce, odpovídající činnostem jimi vykonávaným, úkolům jim svěřeným a oprávněním, jimiž disponují. Politika bezpečnosti informací zajišťuje důvěrnost, integritu a dostupnost kritických logických a fyzických aktiv, zdrojů a citlivých údajů platební instituce jak při uložení, tak při přenosu a využívání. S politikou bezpečnosti informací jsou seznámeni všichni pracovníci a externí poskytovatelé.

30. Na základě politiky bezpečnosti informací platební instituce přijme bezpečnostní opatření k omezování rizik IKT a bezpečnosti, jimž je nebo by mohla být vystavena. Opatření pokrývají tyto oblasti:

a) vnitřní správu a řízení v souladu s požadavky podle bodů 10, 11 a 25,

b) logickou bezpečnost,

c) fyzickou bezpečnost,

d) bezpečnost provozu v oblasti informačních a komunikačních technologií,

e) bezpečnostní sledování,

f) přezkumy, hodnocení a testování bezpečnosti informací,

g) odbornou přípravu a informovanost v oblasti bezpečnosti informací.

Logická bezpečnost

31. Platební instituce stanoví, zdokumentuje a uplatňuje postupy pro kontrolu logického přístupu, součástí jsou i kontroly za účelem sledování anomálií. Platební instituce sleduje uplatňování těchto postupů a pravidelně je přezkoumává. Tyto postupy jsou založeny alespoň na těchto zásadách:

a) zásada znalosti pouze potřebného, zásada minimálních oprávnění a zásada oddělenosti funkcí; platební instituce oprávnění přístupu k informačním aktivům a ke svým podpůrným systémům spravuje tak, aby uživatel včetně systémového uživatele (dále jen „uživatel“) věděl jen to, co je potřebné, a to i v případě vzdáleného přístupu; uživatelé mají jen taková přístupová práva, která jsou nezbytně nutná k plnění jejich povinností, s cílem zabránit neoprávněnému přístupu k velkému souboru dat nebo předejít přidělení kombinací přístupových práv, které lze použít k obcházení kontrolních opatření,

b) zásada uživatelské působnosti; platební instituce v co nejvyšší míře omezí používání obecných a sdílených uživatelských účtů a u akcí prováděných v IKT systémech zajistí identifikaci uživatele,

c) zásada privilegovaných přístupových oprávnění; platební instituce přísně kontroluje privilegované přístupy do systému pomocí přísného omezení účtů administrátora a dalších účtů se zvýšenými právy přístupu k systému a nad těmito účty zajišťuje důsledný dohled, vzdálený administrativní přístup ke kritickým IKT systémům poskytuje jen tak, aby uživatel věděl jen co je potřebné a jen když se používá silné ověřování identity uživatele,

d) zásada zaznamenávání činnosti uživatele; platební instituce zajistí vedení auditních záznamů a monitorování týkající se alespoň veškerých činností privilegovaných uživatelů, zabezpečení záznamů o přístupu tak, aby se předešlo jejich neoprávněným úpravám nebo výmazu, a jejich uložení po dobu odpovídající kritičnosti identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv; platební instituce tyto informace používá k usnadnění identifikace a vyšetřování neobvyklých činností zjištěných při poskytování služeb,

e) zásada řízení přístupu; platební instituce zajistí, že přístupová práva jsou udělována, odebírána nebo upravována včas, a to podle předem stanovených postupů schvalování zahrnujících vlastníka informačního aktiva, v případě ukončení pracovního poměru nebo obdobného vztahu jsou přístupová práva okamžitě odebrána,

f) zásada revize přístupových oprávnění; platební instituce zabezpečí, že přístupová práva jsou pravidelně přezkoumávána s cílem zajistit, aby uživatelé nepožívali nadměrných výsad a aby byla přístupová práva odebrána, jakmile již nebudou zapotřebí,

g) zásada odpovídajících autentizačních metod; platební instituce prosazuje metody ověření, které jsou dostatečně robustní, aby přiměřeně a účinně zajistily dodržování zásad a postupů kontroly přístupu, odpovídají kritičnosti IKT systémů, informací nebo procesů, k nimž se přistupuje, zahrnují přinejmenším složitá hesla, dvoufaktorová ověření nebo jiné silné metody ověření, a to podle příslušného rizika.

32. Platební instituce zajistí, že vzdálený přístup prostřednictvím aplikací k datům a IKT systémům je omezen na minimum, které je nutné k poskytování příslušné služby.

Fyzická bezpečnost

33. Platební instituce stanoví, zdokumentuje a uplatňuje opatření pro fyzické zabezpečení platební instituce k zajištění ochrany jejích prostor, datových center a citlivých oblastí před neoprávněným přístupem a před riziky okolního prostředí.

34. Platební instituce zajistí, že fyzický přístup k IKT systémům je povolen pouze oprávněným osobám, oprávnění je přiděleno v souladu s úkoly a povinnostmi dotčené osoby a je omezeno na osoby, které jsou řádně vyškoleny a jejichž činnosti jsou monitorovány. Platební instituce zajistí, že fyzický přístup je pravidelně přezkoumáván a v případě potřeby jsou nepotřebná přístupová práva zrušena.

35. Platební instituce přijme přiměřená opatření na ochranu před riziky okolního prostředí, která jsou úměrná důležitosti budov a kritičnosti operací nebo IKT systémů umístěných v těchto budovách.

Bezpečnost provozu v oblasti informačních a komunikačních technologií

36. Platební instituce stanoví, zdokumentuje a uplatňuje postupy, které zamezují výskytu bezpečnostních incidentů v IKT systémech a IKT službách, a minimalizuje jejich dopad na poskytování těchto služeb. Tyto postupy zahrnují

    a) identifikace potenciálních zranitelností, které jsou vyhodnoceny a napraveny aktualizací softwaru a firmwaru, včetně softwaru, který platební instituce poskytuje uživatelům, provedením kritických bezpečnostních oprav nebo zavedením kompenzačních opatření,

    b) zavedení požadavků na zabezpečení základní konfigurace všech síťových komponent,

    c) zavedení segmentace sítě, systémů prevence ztráty dat a šifrování síťového provozu, a to v souladu s klasifikací dat,

    d) zavedení ochrany koncových bodů včetně serverů, pracovních stanic a mobilních zařízení; dříve než bude těmto bodům umožněn přístup do podnikové sítě, platební instituce vyhodnocuje, zda koncové body splňují jí vymezené bezpečnostní standardy,

    e) zavedení mechanismů pro ověření integrity softwaru, firmwaru a dat,

    f) šifrování uložených a přenášených dat, a to v souladu s klasifikací dat.

37. Platební instituce průběžně zjišťuje, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření za účelem zmírnění rizik. Platební instituce zajistí, že tyto změny jsou řádně naplánovány, otestovány, zdokumentovány, schváleny a zavedeny.

Bezpečnostní sledování

38. Platební instituce provádí průběžné bezpečnostní sledování. K tomu si stanoví, zdokumentuje a uplatňuje postupy pro odhalování neobvyklých činností, které mohou mít dopad na bezpečnost informací platební instituce, a pro reagování na tyto události. V rámci průběžného bezpečnostního sledování je platební instituce schopna odhalovat a ohlašovat fyzická nebo logická narušení a porušení důvěrnosti, integrity a dostupnosti informačních aktiv. Platební instituce se zaměřuje na

    a) relevantní vnitřní a vnější faktory, včetně obchodních funkcí a administrativních funkcí v oblasti informačních a komunikačních technologií,

    b) transakce, aby bylo možné odhalit zneužití přístupu třetí stranou nebo uvnitř platební instituce,

    c) potenciální vnitřní a vnější hrozby.

39. Platební instituce má organizační uspořádání, které jí umožňuje identifikovat a soustavně sledovat bezpečnostní hrozby s podstatným vlivem na její schopnost poskytovat služby. Platební instituce aktivně sleduje technologický vývoj, aby si byla vědoma rizik bezpečnosti. Platební instituce uplatňuje opatření zejména k identifikaci možných úniků informací, škodlivých kódů a dalších bezpečnostních hrozeb a veřejně známých zranitelností softwaru a hardwaru a kontroluje odpovídající nové aktualizace zabezpečení.

40. Bezpečnostní sledování platební instituci pomáhá pochopit povahu bezpečnostních a provozních incidentů, identifikovat trendy a podporovat jí prováděné vyšetřování.

Přezkumy, hodnocení a testování bezpečnosti informací

41. Platební instituce uplatňuje pro přezkumy, hodnocení a testování bezpečnosti informací různé postupy a nástroje tak, aby zajistila účinnou identifikaci zranitelností v IKT systémech a IKT službách, a to pomocí diferenční analýzy oproti standardům bezpečnosti informací nebo jiným způsobem, přezkumy dodržování předpisů, audity informačních systémů a kontroly fyzického zabezpečení. Platební instituce zvažuje další osvědčené postupy, jako jsou přezkumy zdrojového kódu, hodnocení zranitelností, penetrační testy a cvičení simulující reálný průnik do IKT systémů.

42. Platební instituce stanoví a uplatňuje rámec pro testování bezpečnosti informací, který ověřuje spolehlivost a účinnost jejích opatření v oblasti bezpečnosti informací, zohledňuje hrozby a zranitelnosti identifikované prostřednictvím sledování hrozeb a vyhodnocování rizik IKT a bezpečnosti.

43. Rámec pro testování bezpečnosti informací zajišťuje, že testy

    a) provádějí nezávislé osoby odborně způsobilé, které mají dostatečné zkušenosti v oblasti testování opatření pro bezpečnost informací a nepodílí se na vývoji opatření pro bezpečnost informací,

    b) zahrnují kontroly zranitelností a případně penetrační testy, včetně penetračního testování na základě hrozeb, je-li to nutné a vhodné, úměrné úrovni rizika rozpoznaného u obchodních procesů a systémů.

44. Platební instituce provádí průběžné a opakované testy bezpečnostních opatření. Testy u všech kritických IKT systémů provádí alespoň jednou ročně a jsou součástí komplexního vyhodnocení bezpečnostních a provozních rizik v souvislosti s poskytováním služeb, o němž platební instituce informuje Českou národní banku podle § 222 odst. 1 zákona. Jiné než kritické systémy platební instituce testuje pravidelně na základě přístupu založeného na riziku, alespoň však každé tři roky.

45. Platební instituce zajistí, že testy bezpečnostních opatření se provádí v případě změn infrastruktury, procesů nebo postupů a v případě, že dojde ke změnám v důsledku závažných bezpečnostních a provozních incidentů nebo v důsledku vydání nových nebo výrazně změněných kritických aplikací přímo dostupných z internetu.

46. Platební instituce sleduje a vyhodnocuje výsledky bezpečnostních testů a odpovídajícím způsobem aktualizuje svá bezpečnostní opatření, v případě kritických IKT systémů bez zbytečného odkladu.

47. Platební instituce uplatňuje také bezpečnostní opatření týkající se

    a) platebních terminálů a zařízení používaných k poskytování platebních služeb,

    b) platebních terminálů a zařízení používaných k ověřování uživatelů platebních služeb,

    c) zařízení a softwaru poskytovaných uživatelům za účelem vygenerování nebo jiné formy získání ověřovacího kódu.

48. Platební instituce na základě zjištěných bezpečnostních hrozeb a uskutečněných změn provádí testy, které zahrnují scénáře relevantních a známých potenciálních útoků.

Odborná příprava a povědomí týkající se bezpečnosti informací

49. Platební instituce zavede program odborné přípravy zahrnující pravidelné programy zvyšování povědomí v oblasti bezpečnosti pro všechny pracovníky a externí poskytovatele a zajistí, že pracovníci a externí poskytovatelé jsou vyškoleni k plnění svých úkolů a povinností v souladu s příslušnými bezpečnostními zásadami a postupy, jejichž cílem je odstranit lidské chyby, krádeže, podvodná jednání, zneužití nebo ztráty a řešit rizika spojená s bezpečností informací. Platební instituce zajistí, aby program odborné přípravy zajišťoval školení pro všechny pracovníky a externí poskytovatele alespoň jednou ročně.

Řízení provozu v oblasti informačních a komunikačních technologií

50. Platební instituce řídí provoz v oblasti informačních a komunikačních technologií na základě zdokumentovaných a zavedených procesů a postupů, které schvaluje vedoucí pracovník. Tento soubor dokumentů vymezuje, jak platební instituce provozuje, sleduje a kontroluje své IKT systémy a IKT služby, jak dokumentuje kritické operace v oblasti informačních a komunikačních technologií, jak udržuje aktuální soupis softwaru a hardwaru, který se nachází v obchodním prostředí (dále jen „IKT aktivum“).

51. Platební instituce zajistí, aby výkonost provozu v oblasti informačních a komunikačních technologií byla v souladu s jejími provozními požadavky. Platební instituce udržuje a pokud možno zvyšuje účinnost provozu v oblasti informačních a komunikačních technologií, včetně zvažování, jak minimalizovat možné chyby vznikající při provádění manuálních úkolů.

52. Platební instituce stanoví a uplatňuje u kritických částí provozu v oblasti informačních a komunikačních technologií postupy logování a sledování, které umožňují odhalit, analyzovat a opravovat chyby.

53. Platební instituce udržuje aktuální soupis IKT aktiv včetně síťových zařízení a databází. Soupis těchto aktiv uchovává jejich konfiguraci i vazby a vzájemné závislosti mezi nimi pro správný proces konfigurace a řízení změn.

54. Soupis IKT aktiv je dostatečně podrobný, aby umožnil okamžitou identifikaci takového aktiva, jeho umístění, bezpečnostní klasifikaci a osobu, která ho má v působnosti. Platební instituce má zdokumentovány vzájemné vazby mezi IKT aktivy kvůli schopnosti reagovat na bezpečnostní a provozní incidenty, včetně kybernetických útoků.

55. Platební instituce sleduje a řídí životní cykly IKT aktiv, aby zajistila, že tato aktiva budou i nadále splňovat a podporovat požadavky týkající se obchodní činnosti i řízení rizik. Platební instituce sleduje, zda její IKT aktiva jsou podporována vývojáři i externími poskytovateli a zda jsou všechny příslušné opravy a aktualizace prováděny na základě zdokumentovaných procesů. Platební instituce vyhodnocuje a omezuje rizika vyplývající ze zastaralých nebo nepodporovaných IKT aktiv.

56. Platební instituce stanoví a uplatňuje procesy plánování a sledování výkonnosti IKT systémů a zajišťuje kapacity tak, aby včas předešla závažným problémům s jejich výkonností a nedostatkem v jejich kapacitě, včas je zjišťovala a reagovala na ně.

57. Platební instituce stanoví a uplatňuje postupy zálohování a obnovy dat a IKT systémů, aby tato data a systémy byla schopna v případě potřeby obnovit. Rozsah

a četnost zálohování stanoví podle požadavků na obnovení činnosti a kritičnosti dat a IKT systémů a hodnotí ji podle provedeného vyhodnocení rizik. Platební instituce pravidelně provádí testování postupů zálohování a obnovy dat a IKT systémů.

58. Platební instituce zajistí, aby zálohy dat a IKT systémů byly bezpečně uloženy a dostatečně vzdáleny od primárního místa tak, aby nebyly vystaveny stejným rizikům.

Řízení incidentů a problémů v oblasti informačních a komunikačních technologií

59. Platební instituce stanoví a uplatňuje proces řízení incidentů a problémů pro sledování a zaznamenávání bezpečnostních a provozních incidentů v oblasti informačních a komunikačních technologií, aby co nejdříve pokračovala nebo obnovila kritické obchodní funkce a procesy v případě narušení. Platební instituce stanoví příslušná kritéria a prahové hodnoty ke klasifikaci události jako bezpečnostního nebo provozního incidentu a indikátory včasného varování, které zajišťují včasné odhalení incidentů. Platební instituce při tom uplatňuje klasifikaci významných incidentů podle Obecných pokynů Evropského orgánu pro bankovnictví k oznamování významných incidentů podle směrnice (EU) 2015/2366 o platebních službách na vnitřním trhu (PSD2).

60. K zajištění minimalizace dopadů nepříznivých událostí a umožnění včasné obnovy platební instituce stanoví a uplatňuje vhodné postupy a má vhodné organizační uspořádání, které zajistí jednotné a integrované sledování, řešení a návazné sledování bezpečnostních a provozních incidentů a zabezpečí, aby byly identifikovány a odstraněny jejich hlavní příčiny a zamezeno výskytu opakovaných incidentů. Postupy řízení incidentů a problémů zahrnují

a) postupy pro rozpoznávání, zpětné sledování, zaznamenávání, kategorizaci a klasifikaci incidentů podle priority na základě kritičnosti z hlediska obchodní činnosti,

b) role a povinnosti pro různé scénáře v případě chyb, poruch, kybernetických útoků a jiných incidentů,

c) postupy pro identifikaci, analýzu a řešení hlavní příčiny jednoho nebo více incidentů, přičemž platební instituce

1. analyzuje bezpečnostní a provozní incidenty s pravděpodobným vlivem na ni, které byly identifikovány nebo se vyskytly uvnitř nebo vně platební instituce,

2. zohledňuje hlavní zjištění z těchto analýz a odpovídajícím způsobem aktualizuje bezpečnostní opatření,

d) účinné plány vnitřní komunikace včetně postupů pro oznamování incidentů a jejich předání na vyšší úroveň řízení, zahrnující i stížnosti uživatelů platebních služeb související s bezpečností, přičemž tyto postupy zajišťují, že

1. incidenty s potenciálně velkým nepříznivým dopadem na kritické IKT systémy a IKT služby jsou oznamovány příslušné osobě s působností v oblasti informačních a komunikačních technologií a vedoucímu pracovníkovi,

2. v případě závažných incidentů jsou informováni vedoucí osoby a vedoucí pracovník, a to alespoň o dopadu, reakci a dodatečných kontrolách, které platební instituce stanoví na základě vyhodnocení incidentů,

e) postupy reakce na incidenty ke zmírnění dopadů souvisejících s incidenty a zajištění včasného obnovení činnosti a bezpečnosti služby,

f) specifické plány vnější komunikace pro kritické obchodní funkce a procesy, které platební instituci umožní spolupracovat s příslušnými zainteresovanými osobami za účelem účinné reakce na incident a obnovy po incidentu a poskytnout včasné informace uživatelům platebním služeb a jiným třetím stranám.

Řízení projektů v oblasti informačních a komunikačních technologií

61. Platební instituce uskutečňuje program nebo proces správy a řízení projektů, který vymezí role, povinnosti a působnosti pro účinnou podporu provádění strategie v oblasti informačních a komunikačních technologií. Projekty v oblasti informačních a komunikačních technologií jsou používány v případě výměny, náhrady, likvidace nebo zavádění IKT systémů a IKT služeb. Tyto projekty mohou být součástí širších programů transformace v oblasti informačních a komunikačních technologií nebo obchodní činnosti.

62. Platební instituce náležitě sleduje a omezuje rizika vyplývající z jejího portfolia projektů v oblasti informačních a komunikačních technologií a zohledňuje také rizika, která mohou vyplývat ze vzájemných vazeb mezi různými projekty a z vazeb více projektů na týchž zdrojích nebo odborných znalostech.

63. Platební instituce stanoví a uplatňuje politiku řízení projektů v oblasti informačních a komunikačních technologií, která zahrnuje alespoň

a) cíle projektu,

b) role a povinnosti v projektu,

c) vyhodnocení rizik projektu,

d) plán, časový rámec a fáze projektu,

e) hlavní mezníky projektu,

f) požadavky týkající se řízení změn.

64. Politika řízení projektů v oblasti informačních a komunikačních technologií zajišťuje, aby požadavky na bezpečnost informací byly analyzovány a schváleny funkcí, která je nezávislá na funkci vývoje.

65. Platební instituce zajistí, aby v projektovém týmu byly zastoupeny všechny oblasti ovlivněné projektem v oblasti informačních a komunikačních technologií. Projektový tým musí mít znalosti potřebné k zajištění bezpečné a efektivní realizace projektu a jeho dokončení.

66. Vedoucí pracovník je informován o přípravě, zahájení a postupu projektů v oblasti informačních a komunikačních technologií a s nimi souvisejících rizicích, a to jednotlivě nebo souhrnně za všechny projekty, podle významu a velikosti projektů v oblasti informačních a komunikačních technologií, pravidelně a podle potřeby také jednorázově. Platební instituce zahrnuje riziko projektů do svého systému řízení rizik.

Pořizování a vývoj IKT systémů

67. Platební instituce stanoví a uplatňuje postup pro pořízení, vývoj a údržbu IKT systémů. Uplatňuje přitom rizikově orientovaný přístup.

68. Platební instituce zajistí, aby před provedením jakéhokoli pořízení nebo vývoje IKT systémů příslušné úrovně vedení srozumitelně vymezily a schválily požadavky, včetně funkčních požadavků a požadavků na bezpečnost informací.

69. Platební instituce stanoví a uplatňuje opatření k omezení rizika neúmyslné nebo úmyslné změny IKT systémů během vývoje a zavádění v produkčním prostředí.

70. Platební instituce stanoví a uplatňuje postupy pro testování a schvalování IKT systémů před jejich prvním použitím. Tyto postupy zohledňují kritičnost obchodních procesů a aktiv. Testování zajišťuje, aby nové IKT systémy fungovaly tak, jak bylo zamýšleno. Platební instituce také používá testovací prostředí, které přiměřeně odráží její produkční prostředí.

71. Platební instituce testuje IKT systémy, IKT služby a opatření pro bezpečnost informací tak, aby identifikovala možná slabá místa, narušení a incidenty v oblasti bezpečnosti.

72. Platební instituce zavede samostatná prostředí informačních a komunikačních technologií, aby zajistila odpovídající oddělení funkcí a omezila dopad neověřených změn na produkční systémy. Platební instituce zajistí oddělení produkčních prostředí od vývojových, testovacích a ostatních neprodukčních prostředí. Platební instituce zajistí integritu a důvěrnost produkčních dat v neprodukčních prostředích. Přístup k datům z produkčního prostředí platební instituce omezí na oprávněné uživatele.

73. Platební instituce stanoví a uplatňuje opatření na ochranu integrity zdrojových kódů IKT systémů, které jsou vyvíjeny uvnitř platební instituce. Platební instituce komplexně zdokumentuje vývoj, zavádění, provoz a konfiguraci IKT systémů, aby se snížila jakákoli nadbytečná závislost na odbornících v dané oblasti. Dokumentace IKT systémů obsahuje alespoň uživatelskou dokumentaci, dokumentaci technického systému a provozní postupy.

74. Postupy platební instituce pro pořízení a vývoj IKT systémů zahrnují také IKT systémy vyvinuté nebo řízené obchodními funkcemi a koncovými uživateli mimo organizaci v oblasti informačních a komunikačních technologií. Platební instituce přitom uplatní rizikově orientovaný přístup. Platební instituce vede evidenci aplikací, které podporují kritické obchodní funkce nebo procesy.

Řízení změn v oblasti informačních a komunikačních technologií

75. Platební instituce stanoví a uplatňuje proces řízení změn v oblasti informačních a komunikačních technologií, aby zajistila, že všechny změny IKT systémů jsou zaznamenávány, testovány, posuzovány, schvalovány, prováděny a ověřovány kontrolovaným způsobem. Platební instituce zpracuje změny během mimořádných událostí, zavedené bez zbytečného odkladu, podle postupů, které zajistí dostatečnou spolehlivost.

76. Platební instituce průběžně zjišťuje, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření k omezení rizik. Tyto změny jsou v souladu s procesem, který platební instituce stanovila a uplatňuje pro řízení změn.

Řízení kontinuity činnosti

77. Platební instituce stanoví a uplatňuje řádný proces pro zajištění plynulého výkonu činností a trvalého fungování platební instituce (dále jen „řízení kontinuity

činnosti“), aby upevnila svou schopnost poskytovat dále služby a omezila ztráty v případě závažného narušení podnikatelské činnosti.

78. V rámci řádného řízení kontinuity činnosti platební instituce analyzuje dopad na podnikatelskou činnost posuzováním své expozice vůči závažným narušením činnosti a jejich možným dopadům, včetně dopadů v oblasti důvěrnosti, integrity a dostupnosti, a to kvantitativně i kvalitativně. Využívá vnitřních údajů, údajů externích poskytovatelů významných pro obchodní proces, veřejně dostupných údajů nebo jiných vnějších údajů, které mohou být z hlediska analýzy dopadu na podnikatelskou činnost relevantní, a analýzu scénářů. Platební instituce v analýze dopadu na podnikatelskou činnost také zvažuje kritičnost identifikovaných a klasifikovaných obchodních funkcí, podpůrných procesů, třetích stran a informačních aktiv a jejich vzájemné vazby.

79. Platební instituce zajistí, aby její IKT systémy a IKT služby byly navrženy a sladěny s její analýzou dopadu na podnikatelskou činnost, zejména jde-li o redundanci určitých kritických komponent, aby se zamezilo narušení způsobenému událostmi, které mají na tyto složky dopad.

80. Platební instituce na základě svých analýz dopadu na podnikatelskou činnost vypracuje plány kontinuity činnosti, které jsou zdokumentovány a schváleny vedoucím pracovníkem. Plány kontinuity činnosti zohledňují zejména rizika, která by mohla mít nepříznivý dopad na IKT systémy a IKT služby. Plány kontinuity činnosti podporují cíle týkající se ochrany a v případě potřeby obnovy důvěrnosti, integrity a dostupnosti obchodních funkcí, podpůrných procesů a informačních aktiv. Platební instituce při sestavování plánů kontinuity činnosti podle potřeby koordinuje svou činnost uvnitř platební instituce i se zainteresovanými třetími stranami.

81. Platební instituce má plány kontinuity činnosti, aby zajistila, že bude moci přiměřeně reagovat na případné scénáře selhání a že bude schopna obnovit provoz svých kritických obchodních činností po přerušení v rámci maximální doby, během níž musí být po incidentu obnoven systém nebo proces (dále jen „cílová doba obnovy“) a v rámci maximální lhůty, během níž je přijatelná ztráta dat v případě incidentu (dále jen „cílový bod obnovy“). V případě vážného narušení činnosti, které aktivuje konkrétní plány kontinuity činnosti, platební instituce stanoví přednost opatření pro kontinuitu činnosti na základě rizikově orientovaného přístupu.

82. Platební instituce ve svém plánu kontinuity činnosti zvažuje různé scénáře, včetně méně pravděpodobných scénářů vývoje, kterému může být vystavena, a to včetně scénáře kybernetického útoku. Platební instituce posuzuje možný dopad naplnění takových scénářů. Na základě těchto scénářů platební instituce stanoví, jak by byla zajištěna kontinuita IKT systémů a IKT služeb, jakož i bezpečnost informací platební instituce.

83. Platební instituce na základě analýz dopadu na podnikatelskou činnost a věrohodných scénářů vypracuje plány reakce a obnovy činnosti platební instituce. Tyto plány specifikují, jaké podmínky mohou urychlit aktivaci plánů a jaká opatření musí být přijata k zajištění dostupnosti, kontinuity a obnovy přinejmenším kritických IKT systémů a IKT služeb provozovaných platební institucí.

84. Plány reakce a obnovy zohledňují krátkodobé i dlouhodobé možnosti obnovy. Tyto plány jsou

a) zaměřeny na obnovu činnosti kritických obchodních funkcí, podpůrných procesů, informačních aktiv a jejich vzájemných vazeb, aby bylo zamezeno nepříznivým dopadům na fungování platební instituce a na platební systém, včetně dopadů na platební systémy a na uživatele platebních služeb, a zajištěno provedení čekajících platebních transakcí,

b) jsou zdokumentovány a zpřístupněny obchodním a podpůrným útvarům a jsou snadno dostupné v případě mimořádné situace,

c) jsou aktualizovány v souladu s poznatky získanými z incidentů, testování, s nově identifikovanými riziky či hrozbami a se změněnými cíli a prioritami obnovy.

85. Plány reakce a obnovy také zohledňují alternativní možnosti v případech, kdy obnova nemusí být z krátkodobého hlediska proveditelná z důvodu nákladů, rizik, logistiky nebo nepředvídaných okolností.

86. V rámci plánů reakce a obnovy platební instituce vezme v potaz opatření pro kontinuitu činnosti ke zmírnění selhání externích poskytovatelů, kteří mají klíčový význam pro kontinuitu IKT služeb platební instituce, a to přiměřeně v souladu s Obecnými pokyny k outsourcingu vydanými Evropským orgánem pro bankovnictví.

87. Platební instituce plány kontinuity činnosti pravidelně testuje. Zejména zajistí, aby plány kontinuity činnosti jejích kritických obchodních funkcí, podpůrných procesů, informačních aktiv a jejich vzájemných vazeb, včetně těch funkcí, procesů a aktiv, které případně poskytly třetí strany, byly testovány alespoň jednou ročně.

88. Platební instituce vyhodnocuje nutnost aktualizace plánů kontinuity činnosti alespoň jednou ročně na základě výsledků testování, aktuálních informací o hrozbách a zkušeností získaných z předchozích událostí. Jakékoli změny cílů obnovy, včetně změn cílové doby obnovy a cílového bodu obnovy, nebo změny obchodních funkcí, podpůrných procesů a informačních aktiv jsou náležitě zohledněny jako vstup do aktualizace plánů kontinuity činnosti.

89. Testováním plánů kontinuity činnosti platební instituce prokáže, že je schopna zachovat své činnosti do doby obnovy kritické operace. Platební instituce zejména

a) zahrnuje testování vhodného souboru závažných, ale pravděpodobných scénářů, včetně scénářů zvažovaných pro vývoj plánů kontinuity činnosti, a případně testování služeb poskytovaných třetími stranami; součástí je převod kritických obchodních funkcí, podpůrných procesů a informačních aktiv do prostředí pro obnovu po havárii a prokázání toho, že je lze takto provozovat po dostatečné časové období a poté lze obnovit obvyklou činnost,

b) navrhuje testování tak, aby prověřilo předpoklady, na nichž jsou založeny plány kontinuity činnosti, včetně systémů správy a řízení a plánů krizové komunikace, a

c) zahrnuje postupy k ověření schopnosti pracovníků a externích poskytovatelů, IKT systémů a IKT služeb provozovaných platební institucí přiměřeně reagovat na scénáře podle písmene a).

90. Platební instituce zajistí, že výsledky testů jsou zdokumentovány a veškeré zjištěné nedostatky vyplývající z testů jsou analyzovány, řešeny a oznámeny vedoucímu pracovníkovi.

91. Pro případy narušení nebo mimořádné situace a během provádění plánů kontinuity činnosti platební instituce zajistí, aby byla stanovena a uplatňována účinná komunikační opatření pro případ krize, aby byly včas a vhodným způsobem informovány všechny příslušné osoby uvnitř platební instituce, uživatelé platebních služeb i jiné zainteresované třetí strany, včetně příslušných vnitrostátních orgánů, pokud to vyžadují právní předpisy, a příslušní externí poskytovatelé.

Řízení vztahů s uživateli platebních služeb

92. Platební instituce stanoví a uplatňuje postupy pro zvýšení povědomí uživatelů platebních služeb o bezpečnostních rizicích spojených s platebními službami, a to prostřednictvím asistenčních služeb a poradenství pro uživatele platebních služeb.

93. Platební instituce zajistí, že asistenční služby a poradenství nabízené uživatelům platebních služeb jsou aktualizovány s ohledem na nové hrozby a zranitelnosti a uživatelé platebních služeb jsou o všech změnách informováni.

94. Umožňuje-li to funkčnost produktu, platební instituce umožní uživatelům platebních služeb deaktivovat konkrétní platební funkce, které souvisí s platebními službami nabízenými uživateli platebních služeb.

95. Pokud se platební instituce dohodla s uživatelem platebních služeb na omezeních podle § 163 zákona, umožňuje uživateli platebních služeb tento stanovený maximální limit upravit.

96. Platební instituce poskytuje uživatelům platebních služeb možnost dostávat upozornění o provedených nebo neúspěšných pokusech o zadání příkazu k platební transakci a tím jim umožňuje odhalit podvodné nebo neoprávněné používání jejich účtů.

97. Platební instituce informuje uživatele platebních služeb o aktuálních změnách bezpečnostních postupů, které mají vliv na poskytování platebních služeb uživateli platebních služeb.

98. Platební instituce poskytuje uživatelům platebních služeb pomoc v případě jakéhokoli dotazu, žádosti o podporu a oznámení anomálií nebo potíží týkajících se bezpečnostních záležitostí, které se vztahují na platební služby. Platební instituce uživatele platebních služeb náležitě informuje o tom, jak mohou tuto pomoc získat.“.

Čl. II

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. července 2022.

Guvernér:

Ing. **Rusnok** v. r.