Třídicí znak							
2	2	1	2	1	5	6	0

ÚŘEDNÍ SDĚLENÍ ČESKÉ NÁRODNÍ BANKY

ze dne 20. prosince 2021

k hlášení bezpečnostních a provozních incidentů v oblasti platebního styku

Ustanovení § 221 odst. 1 zákona č. 370/2017 Sb., o platebním styku, v platném znění (dále jen „zákon“) stanoví, že osoba oprávněná poskytovat platební služby oznámí orgánu dohledu domovského členského státu závažný bezpečnostní nebo provozní incident v oblasti platebního styku bez zbytečného odkladu po jeho zjištění.

Česká národní banka k § 221 odst. 1 zákona sděluje:

I.
Klasifikace incidentů jako závažných

1. Osoby oprávněné poskytovat platební služby (dále též „oznamující osoby“) by měly jako závažné klasifikovat bezpečnostní a provozní incidenty, které splňují

   a. alespoň jedno z kritérií na „vyšší úrovni dopadu“ nebo
   b. alespoň tři z kritérií na „nižší úrovni dopadu“

   vymezených v části I bodu 4 a na základě posouzení podle tohoto úředního sdělení.

2. Oznamující osoby by měly posoudit bezpečnostní a provozní incident na základě následujících kritérií a souvisejících ukazatelů:

   i. Dotčené transakce

   Oznamující osoby by měly určit celkovou hodnotu dotčených platebních transakcí i počet zasažených transakcí vyjádřený jako procentuální podíl běžné úrovně platebních transakcí prováděných jimi v rámci poskytování dotčených platebních služeb.

   ii. Dotčení uživatelé platebních služeb

   Oznamující osoby by měly určit počet svých dotčených uživatelů platebních služeb, a to v absolutním vyjádření i jako procentuální podíl z celkového počtu svých uživatelů platebních služeb.

   iii. Narušení zabezpečení sítě nebo informačních systémů

   Oznamující osoby by měly rozhodnout, zda nějaká škodlivá činnost narušila zabezpečení sítě nebo informačních systémů souvisejících s poskytováním platebních služeb.

   iv. Délka výpadku služby

   Oznamující osoby by měly určit dobu, po kterou bude služba uživateli platební služby pravděpodobně nedostupná nebo po kterou oznamující osoba nebude moci provést platební příkaz.

   v. Ekonomický dopad

   Oznamující osoby by měly uceleně určit výši nákladů souvisejících s incidentem a zohlednit jejich absolutní výši a případně relativní význam těchto nákladů v poměru k výši svého kapitálu tier 1.

vi. Vysoká úroveň interní eskalace

Oznamující osoby by měly rozhodnout, zda tento incident byl nebo pravděpodobně bude nahlášen jejich vedoucí osobě.

vii. Ostatní potenciálně dotčené oznamující osoby nebo příslušné infrastruktury

Oznamující osoby by měly určit systémové důsledky, které incident pravděpodobně bude mít, tj. jeho potenciální rozšíření mimo oznamující osobu mezi další osoby oprávněné poskytovat platební služby, infrastruktury finančního trhu nebo schémata platebních karet[1].

viii. Reputační dopad

Oznamující osoby by měly vyhodnotit, zda a jak může incident ohrozit důvěru, kterou v ně uživatelé mají, a obecněji v související službu nebo trh jako celek.

3. Oznamující osoby by měly vypočítat hodnotu ukazatelů pomocí následující metodiky:

i. Dotčené platební transakce

Oznamující osoby by obecně měly chápat jako „dotčené platební transakce“ veškeré vnitrostátní a přeshraniční platební transakce, které incidentem byly nebo pravděpodobně budou přímo nebo nepřímo dotčeny, a zejména pak platební transakce, které nebylo možné iniciovat nebo zpracovat, platební transakce, u kterých došlo k pozměnění obsahu platební zprávy[2], a platební transakce, k nimž byl příkaz zadán podvodně (bez ohledu na to, zda peněžní prostředky byly či nebyly získány zpět), nebo jejichž řádné provedení je incidentem znemožněno nebo jinak ztíženo.

U provozních incidentů, které ovlivňují schopnost iniciovat a/nebo zpracovávat platební transakce, by oznamující osoby měly hlásit pouze ty incidenty, které trvají déle než jednu hodinu. Doba trvání incidentu by měla být měřena od okamžiku vzniku incidentu do okamžiku obnovení běžných činností či operací na takovou úroveň, na které byly vykonávány před incidentem.

Oznamující osoby by měly za běžnou úroveň platebních transakcí považovat denní průměr vnitrostátních a přeshraničních platebních transakcí provedených v rámci jednotlivých platebních služeb za předchozí rok, které byly incidentem dotčeny. Jestliže oznamující osoby tento údaj nepovažují za vypovídající (např. kvůli sezónnosti), měly by místo toho použít jiný, více vypovídající údaj a sdělit České národní bance příslušné odůvodnění tohoto přístupu v odpovídajícím poli formuláře.

ii. Dotčení uživatelé platebních služeb

Oznamující osoby by měly jako „dotčené uživatele platebních služeb“ chápat všechny klienty (vnitrostátní nebo přeshraniční, spotřebitele nebo podnikatele), kteří mají s dotčenou osobou oprávněnou poskytovat platební služby uzavřenu smlouvu, na jejímž základě mají přístup k dotčené platební službě, a kteří pocítili nebo pravděpodobně pocítí důsledky incidentu. Při určování počtu uživatelů platebních služeb, kteří by bývali mohli platební službu využívat během trvání incidentu, by oznamující osoby měly použít odhady vycházející z dřívější činnosti.

U provozních incidentů ovlivňujících schopnost iniciovat a/nebo zpracovávat platební transakce by oznamující osoby měly hlásit pouze ty incidenty, které mají dopad na uživatele platebních služeb a trvají déle než jednu hodinu. Doba trvání incidentu by měla být měřena od okamžiku vzniku incidentu, do okamžiku obnovení běžných činností/operací na takovou úroveň, na které byly vykonávány před incidentem.

Dále by oznamující osoby měly jako celkový počet uživatelů platebních služeb použít souhrnný počet vnitrostátních a přeshraničních uživatelů platebních služeb, kteří jsou s nimi smluvně vázáni v okamžiku incidentu (popřípadě nejaktuálnější dostupný údaj)

[1] Čl. 2 odst. 16 nařízení EP a Rady (EU) 2015/751 o mezibankovních poplatcích za karetní platební transakce
[2] Např. změna částky, měny, jedinečného ukazatele, variabilního či specifického symbolu, nebo data splatnosti, apod.

a mají přístup k dotčené platební službě, bez ohledu na jejich velikost nebo na to, zda jsou považováni za aktivní nebo pasivní uživatele platebních služeb.

iii. Narušení zabezpečení sítě nebo informačních systémů

Oznamující osoby by měly rozhodnout, zda nějaká škodlivá činnost neohrozila dostupnost, autenticitu, integritu nebo důvěrnost sítě nebo informačních systémů (včetně dat) souvisejících s poskytováním platebních služeb.

iv. Délka výpadku služby

Oznamující osoby by měly zohlednit dobu, po kterou trvá nebo pravděpodobně bude trvat výpadek jakékoliv úlohy, procesu nebo kanálu vztahujícího se k poskytování platebních služeb, který znemožňuje i) iniciování a/nebo provedení platební služby nebo ii) přístup k platebnímu účtu. Oznamující osoby by měly určit délku výpadku služby od okamžiku, kdy výpadek začne, přičemž by měly zohlednit dobu, kdy obvykle vykonávají činnosti potřebné pro provedení platebních služeb, a v případě potřeby i dobu, kdy mají zavřeno, ale provádějí údržbu. Ve výjimečných případech, kdy oznamující osoby nemohou určit, kdy výpadek služby začal, měly by počítat délku výpadku služby od okamžiku, kdy byl výpadek zjištěn.

v. Ekonomický dopad

Oznamující osoby by měly zohlednit náklady přímo související s incidentem i náklady, které se k incidentu vztahují nepřímo. Oznamující osoby by měly mimo jiné vzít v úvahu odcizené peněžní prostředky nebo aktiva, náklady na výměnu hardwaru nebo softwaru, další náklady na forenzní analýzy nebo zvládnutí incidentu, poplatky v důsledku nedodržení smluvních povinností, sankce, externí závazky a ušlé výnosy. Pokud jde o nepřímé náklady, oznamující osoby by měly zohlednit pouze ty, které jsou již známy nebo které velmi pravděpodobně vzniknou.

vi. Vysoká úroveň interní eskalace

Oznamující osoby by měly zvážit, zda v důsledku dopadu na služby související s platbami[3] byl, nebo pravděpodobně bude o incidentu informován vedoucí orgán[4], a to mimo jakýkoli postup pravidelného oznamování zaznamenaných incidentů[5], a průběžně po celou dobu trvání incidentu.

Dále by oznamující osoby měly zohlednit, zda v důsledku dopadu incidentu na služby související s platbami byl nebo pravděpodobně bude vyhlášen krizový režim.

vii. Ostatní potenciálně dotčené osoby oprávněné poskytovat platební služby nebo příslušné infrastruktury

Oznamující osoby by měly posoudit dopad incidentu na infrastruktury finančního trhu, platební schémata je podporující a další osoby oprávněné poskytovat platební služby. Oznamující osoby by měly zejména posoudit, zda se incident projevil nebo se pravděpodobně projeví u jiných osob oprávněných poskytovat platební služby, zda ovlivnil nebo pravděpodobně ovlivní hladké fungování infrastruktur finančního trhu a zda ohrozil nebo pravděpodobně ohrozí řádné fungování finančního systému jako celku. Oznamující osoby by měly zohlednit různé aspekty, například to, zda je dotčená komponenta či dotčený software proprietární nebo všeobecně dostupný, zda je ohrožená síť interní nebo externí a zda oznamující osoba přestala nebo pravděpodobně přestane plnit svoje povinnosti v infrastrukturách finančního trhu, jichž je součástí.

[3] Jakákoliv podnikatelská (obchodní) činnost při poskytování platebních služeb podle § 3 odst. 1 zákona č. 370/2017 Sb., o platebním styku, v platném znění, a všechny technické podpůrné úkoly nezbytné pro jejich správné poskytování.

[4] Jak je definován v obecných pokynech orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti.

[5] V souladu s obecným pokynem 60 písm. d) obecných pokynů orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti: "*účinné plány interní komunikace včetně postupů pro oznamování incidentů a jejich předání na vyšší úroveň řízení (zahrnující i stížnosti zákazníků související s bezpečností), které zajistí:*
i) aby byly incidenty s potenciálně velkým nepříznivým dopadem na kritické systémy IKT a služby v oblasti IKT oznamovány příslušnému vrcholnému vedení a vrcholnému vedení pro IKT;
ii) aby byl v případě závažných incidentů vedoucí orgán informován ad hoc a aby byl vyrozuměn přinejmenším o dopadu, reakci a dodatečných kontrolách, které mají být stanoveny v důsledku incidentů;".

viii. Reputační dopad

Oznamující osoby by měly zvážit úroveň publicity, které incident podle jejich nejlepšího vědomí na trhu dosáhl nebo pravděpodobně dosáhne. Oznamující osoby by měly zvážit zejména pravděpodobnost, že incident bude mít negativní společenský dopad, což je dobrý ukazatel jeho potenciálního dopadu na jejich pověst. Oznamující osoby by měly vzít v úvahu, zda i) si uživatelé platebních služeb nebo jiné osoby oprávněné poskytovat platební služby stěžovaly na nepříznivý dopad incidentu; ii) incident ovlivnil viditelný proces související s platební službou, a je tedy pravděpodobné, že se mu dostane nebo se mu již dostalo mediálního pokrytí (s přihlédnutím nejen k tradičním sdělovacím prostředkům, jako jsou noviny, ale také k blogům, sociálním sítím atd.; mediální pokrytí však v tomto kontextu neznamená pouze několik negativních komentářů sledujících, ale měla by existovat věrohodná zpráva nebo významný počet negativních komentářů či upozornění); iii) došlo nebo pravděpodobně dojde k nedodržení smluvních povinností s následkem zveřejnění právních kroků vůči oznamující osobě; iv) nebyly dodrženy požadavky regulace s následkem uložení dohledových opatření nebo sankcí, které byly nebo pravděpodobně budou zveřejněny; a v) k podobnému druhu incidentu došlo již dříve.

4. Oznamující osoby by měly incident posoudit tak, že u každého jednotlivého kritéria určí, zda před vyřešením incidentu bylo nebo pravděpodobně bude dosaženo příslušných prahových hodnot uvedených v tabulce 1.

Tabulka 1: Prahové hodnoty

Kritéria	Nižší úroveň dopadu	Vyšší úroveň dopadu
Dotčené platební transakce	> 10 % běžné úrovně platebních transakcí oznamující osoby (z hlediska počtu platebních transakcí) **a** doba trvání incidentu > 1 hodina* **nebo** > 500 000 eur **a** doba trvání incidentu > 1 hodina*	> 25 % běžné úrovně platebních transakcí oznamující osoby (z hlediska počtu platebních transakcí) **nebo** > 15 000 000 eur
Dotčení uživatelé platebních služeb	> 5 000 **a** doba trvání incidentu > 1 hodina* **nebo** > 10 % uživatelů platebních služeb oznamující osoby **a** doba trvání incidentu > 1 hodina*	> 50 000 **nebo** > 25 % uživatelů platebních služeb oznamující osoby
Délka výpadku služby	> 2 hodiny	neuplatňuje se
Narušení zabezpečení sítě nebo informačních systémů	ano	neuplatňuje se

Ekonomický dopad	neuplatňuje se	> max (0,1 % kapitálu tier 1**, 200 000 eur) **nebo** > 5 000 000 eur
Vysoká úroveň interní eskalace	ano	ano a pravděpodobně dojde k vyhlášení krizového (nebo podobného) režimu
Ostatní potenciálně dotčené oznamující osoby nebo příslušné infrastruktury	ano	neuplatňuje se
Reputační dopad	ano	neuplatňuje se

* Prahová hodnota týkající se doby trvání incidentu po dobu delší než jedna hodina se vztahuje pouze na provozní incidenty, které ovlivňují schopnost oznamující osoby iniciovat a/nebo zpracovávat platební transakce.
**Kapitál tier 1 ve smyslu článku 25 nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.

5. Pokud nemají k dispozici skutečné údaje, měly by oznamující osoby pro posouzení, zda je nebo pravděpodobně bude dosaženo dané prahové hodnoty před vyřešením incidentu (například ve fázi počátečního šetření), použít odhady.

6. Oznamující osoby by měly toto hodnocení během trvání incidentu provádět průběžně s cílem zjistit případnou možnou změnu klasifikace směrem nahoru (z nezávažného na závažný) nebo směrem dolů (ze závažného na nezávažný). Jakákoli změna klasifikace incidentu ze závažného na nezávažný by měla být bez zbytečného odkladu sdělena České národní bance v souladu s požadavkem v části II. bodu 22.

II.
Způsob oznamování závažných bezpečnostních a provozních incidentů

1. Oznamující osoby by měly shromáždit všechny relevantní informace, vypracovat oznámení o incidentu vyplněním formuláře a oznámení předložit České národní bance. Oznamující osoby by měly všechna pole formuláře vyplnit podle instrukcí uvedených v části VI. tohoto úředního sdělení nazvané „Pokyny k vyplňování oznámení“.

2. Oznamující osoby by měly při předkládání úvodních, průběžných a závěrečných oznámení týkajících se stejného incidentu používat stejný formulář. Oznamující osoby by proto měly postupně vyplňovat pouze jeden formulář a v případě potřeby aktualizovat informace poskytnuté v předchozích oznámeních.

3. Oznamující osoby by měly České národní bance rovněž předložit kopii případných informací pro uživatele podle § 221 odst. 2 zákona, a to jakmile tyto informace jsou k dispozici.

4. Oznamující osoby by měly na základě žádosti České národní banky poskytnout veškeré další dokumenty doplňující informace předložené ve standardizovaném formuláři. Oznamující osoby by měly na základě žádosti České národní banky poskytnout dodatečné informace nebo vysvětlení týkající se již předložené dokumentace.

5. Veškeré další informace obsažené v dokumentech, které oznamující osoby poskytly České národní bance, a to buď z podnětu oznamující osoby, nebo na žádost České národní banky v souladu s částí II. bodem 4, by měly oznamující osoby zohlednit ve formuláři podle části II. bodu 1.

6. Oznamující osoby by měly vždy zachovávat důvěrnost a integritu vyměňovaných informací a řádně prokazovat svou totožnost České národní bance.

7. Česká i anglická verze formuláře v elektronické formě je dostupná na internetových stránkách České národní banky v části Platební styk / Předpisy k platebnímu styku / Úřední sdělení (https://www.cnb.cz/cs/platebni-styk/pravni-predpisy/).

Úvodní oznámení

8. Oznamující osoby by měly České národní bance poté, co byl bezpečnostní nebo provozní incident klasifikován jako závažný, předložit úvodní oznámení. Česká národní banka bez zbytečného odkladu potvrdí e-mailem přijetí úvodního oznámení a přidělí mu ID. Toto ID úvodního oznámení slouží oznamující osobě k vytvoření referenčního kódu jednoznačně identifikujícího incident. Referenční kód se tak skládá z[6]:

   8.1. dvoupísmenného kódu České republiky podle ISO-3166[7], který je tvořen velkými písmeny „CZ“ a uvádí se na začátku referenčního kódu, a od ID úvodního oznámení je oddělen podtržítkem[8], a

   8.2. ID úvodního oznámení, které generuje internetové rozhraní České národní banky pro sběr informačních povinností regulovaných subjektů.

   Oznamující osoby by měly tento referenční kód uvádět při aktualizacích úvodního oznámení, nebo při předkládání průběžných a závěrečných oznámení týkajících se téhož incidentu, pokud nejsou průběžná a závěrečná oznámení předložena společně s úvodním oznámením.

9. Oznamující osoby by měly České národní bance zaslat úvodní oznámení do 4 hodin od okamžiku, kdy byl bezpečnostní nebo provozní incident klasifikován jako závažný, nebo v případě, že internetové rozhraní České národní banky pro sběr informačních povinností a výkazů není v té době dostupné nebo funkční, jakmile se stane dostupným nebo funkčním.

10. Oznamující osoby by měly incident klasifikovat v souladu s částí I. bodem 1 a částí I. bodem 4 bez zbytečného odkladu poté, co mají oznamující osoby k dispozici informace potřebné ke klasifikaci incidentu, nejpozději však do 24 hodin po jeho zjištění. Pokud je ke klasifikaci incidentu zapotřebí delší doba, měly by oznamující osoby v úvodním oznámení předloženém České národní bance vysvětlit důvody, proč byla delší doba zapotřebí.

11. Oznamující osoby by měly úvodní oznámení předložit České národní bance také v okamžiku, kdy je klasifikace incidentu změněna z nezávažného incidentu na závažný. V tomto specifickém případě by oznamující osoby měly úvodní oznámení zaslat České národní bance ihned po zjištění změny stavu nebo v případě, že internetové rozhraní České národní banky pro sběr informačních povinností a výkazů není v té době dostupné nebo funkční, jakmile se stane dostupné nebo funkční.

12. Oznamující osoby by měly v úvodních oznámeních (v oddílu A formuláře), poskytnout informace ze záhlaví, a to včetně základní charakteristiky incidentu a jeho předpokládaných důsledků, a to na základě informací dostupných okamžitě poté, co byl incident klasifikován jako závažný. V případě, že skutečné údaje nejsou k dispozici, měly by oznamující osoby použít odhady.

Průběžné oznámení

13. Oznamující osoby by měly předložit průběžné oznámení po obnovení běžné činnosti a návratu k normálnímu provozu a Českou národní banku o této skutečnosti informovat. Oznamující osoby by měly za návrat k normálnímu provozu považovat situaci, kdy se činnost/provoz navrátí na stejnou úroveň služeb/podmínek, která je stanovena oznamující osobou nebo vymezena externě dohodou o úrovni služeb[9] (z hlediska doby zpracování, kapacity, bezpečnostních požadavků atp.), a kdy již

[6] ČNB upozorňuje, že ID je generováno internetovým rozhraním České národní banky pro sběr informačních povinností regulovaných subjektů při vložení **každého** oznámení, ale pro tvorbu referenčního kódu lze použít jen ID vzniklé z úvodního oznámení.
[7] Dostupné na adrese https://www.iso.org/iso-3166-country-codes.html.
[8] Např. „CZ_R012671397211124135942“.
[9] Tzv. „service-level agreement“.

nejsou zavedena opatření pro nepředvídané události. Průběžné oznámení by mělo obsahovat podrobnější popis incidentu a jeho následků (oddíl B formuláře).

14. Pokud nedošlo k obnovení běžných činností, měly by oznamující osoby předložit České národní bance průběžné oznámení do 3 dnů od předložení úvodního oznámení.

15. Oznamující osoby by měly aktualizovat informace poskytnuté v oddílech A a B formuláře, pokud od předložení předchozího oznámení odhalí významné změny (např. došlo-li k eskalaci nebo ke zmírnění incidentu, nově zjištěné příčiny nebo opatření přijatá k vyřešení problému). To se týká i případů, kdy incident nebyl vyřešen do 3 pracovních dnů; v takovém případě by měly oznamující osoby předložit další (dodatečné) průběžné oznámení. Oznamující osoby by měly další průběžné oznámení předložit rovněž kdykoliv na žádost České národní banky.

16. Stejně jako v případě počátečního oznámení, jestliže nejsou k dispozici skutečné údaje, měly by oznamující osoby použít odhady.

17. Jestliže dojde k návratu k normálnímu provozu do 4 hodin od okamžiku, kdy byl incident klasifikován jako závažný, měly by oznamující osoby usilovat o současné předložení úvodního i průběžného oznámení (tj. vyplnit oddíly A a B formuláře) během uvedené čtyřhodinové lhůty.

Závěrečné oznámení

18. Oznamující osoby by měly závěrečné oznámení předložit po provedení analýzy hlavních příčin (bez ohledu na to, zda již byla přijata opatření ke zmírnění rizik nebo zda již byla zjištěna hlavní příčina), kdy již mají k dispozici skutečné údaje nahrazující případné odhady.

19. Oznamující osoby by měly závěrečné oznámení předložit České národní bance nejpozději do 20 pracovních dnů od návratu k normálnímu provozu. Oznamující osoby, které potřebují tuto lhůtu prodloužit (např. v případě, že ještě nejsou k dispozici skutečné údaje o dopadu nebo zatím nebyly zjištěny hlavní příčiny), by měly kontaktovat Českou národní banku před uplynutím této lhůty a sdělit jí odpovídající důvody zpoždění, jakož i nové předpokládané datum předložení závěrečného oznámení.

20. Jsou-li oznamující osoby schopny poskytnout veškeré informace vyžadované v závěrečném oznámení (tj. v oddíle C formuláře) během uvedené čtyřhodinové lhůty poté, co byl incident klasifikován jako závažný, měly by usilovat o předložení informací vztahujících se k úvodnímu, průběžnému a závěrečnému oznámení najednou.

21. Oznamující osoby by měly v závěrečném oznámení uvést úplné informace, tj. i) skutečné údaje o dopadu namísto odhadů (jakož i případné další potřebné aktualizace v oddílech A a B formuláře) a ii) vyplnit oddíl C formuláře, který obsahuje hlavní příčinu, pokud je již známa, a shrnutí opatření přijatých nebo plánovaných k odstranění problému a zabránění jeho opakování v budoucnu.

22. Oznamující osoby by měly závěrečné oznámení zaslat rovněž v okamžiku, kdy v důsledku průběžného posuzování incidentu zjistí, že oznámený incident již nesplňuje kritéria pro to, aby byl považován za závažný, a předpokládá se, že je před vyřešením již splňovat nebude. V takovém případě by oznamující osoby měly závěrečné oznámení předložit ihned, jakmile je tato skutečnost zjištěna, a v každém případě do lhůty stanovené pro další oznámení. Za této situace by oznamující osoby měly místo vyplnění oddílu C formuláře zvolit pole „změna klasifikace incidentu na nezávažný“ a uvést důvody pro změnu hodnocení závažnosti incidentu.

III.
Přenesené a konsolidované oznamování

Oznamovací povinnosti není možné přenést na třetí osobu (přenesené oznamování). Konsolidované oznamování není možné.

IV.
Bezpečnostní a provozní zásady

Oznamující osoby by měly zajistit, aby jejich obecné bezpečnostní a provozní zásady jasně definovaly veškeré povinnosti související s oznamováním incidentů podle zákona i procesy zavedené s cílem splnit požadavky stanovené v tomto úředním sdělení.

V.
Přepočet na měnu euro

Částky vyjádřené v měně jiné než euro přepočítávají oznamující osoby na euro referenčním směnným kurzem Evropské centrální banky (ECB)[10] pro den předcházející dni předložení oznámení o incidentu (vždy, kdy to připadá v úvahu, tj. u úvodního, jednotlivých průběžných i závěrečného oznámení).

VI.
Pokyny k vyplňování oznámení

INSTRUKCE PRO VYPLNĚNÍ FORMULÁŘE

Oznamující osoby by měly vyplnit příslušný oddíl formuláře v závislosti na fázi oznamování, ve které se nacházejí: oddíl A pro úvodní oznámení, oddíl B pro průběžná oznámení a oddíl C pro závěrečné oznámení. Oznamující osoby by měly při předkládání úvodních, průběžných a závěrečných oznámení týkajících se stejného incidentu používat stejný formulář. Není-li výslovně stanoveno jinak, je třeba vyplnit všechna pole.

Záhlaví

Úvodní oznámení: jedná se o první oznámení, které oznamující osoba předkládá České národní bance.
Průběžné oznámení: obsahuje podrobnější popis incidentu a jeho následků. Jde o aktualizaci úvodního oznámení (a případně předchozího průběžného oznámení) vztahujícího se k témuž incidentu.
Závěrečné oznámení: jedná se o poslední oznámení, které oznamující osoba v souvislosti s incidentem zasílá, neboť i) již byla provedena analýza hlavních příčin a odhady byly nahrazeny skutečnými údaji nebo ii) incident již není považován za závažný a je potřeba změnit jeho klasifikaci.
Změna klasifikace incidentu na nezávažný: incident již nesplňuje kritéria pro to, aby byl považován za závažný, a nepředpokládá se, že je před vyřešením bude splňovat. Oznamující osoby by měly vysvětlit důvody pro tuto změnu klasifikace.
Datum a čas oznámení: přesné datum a čas předložení oznámení České národní bance.
Referenční kód incidentu (používá se u průběžných a závěrečných oznámení a aktualizací úvodního oznámení): referenční kód přidělený Českou národní bankou při předložení úvodního oznámení, který slouží k jednoznačné identifikaci incidentu.

A – Úvodní oznámení

A 1 – Obecné údaje

Druh oznámení:

Individuální: oznámení se vztahuje k jediné osobě oprávněné poskytovat platební služby.

Konsolidované: vzhledem k nemožnosti konsolidovaného oznámení nepřichází vyplnění v úvahu.

Dotčená osoba oprávněná poskytovat platební služby: označuje osobu oprávněnou poskytovat platební služby, u níž k incidentu došlo.

Název osoby oprávněné poskytovat platební služby: celý název osoby oprávněné poskytovat platební služby, jež se oznámení týká, jak je uveden v příslušném úředním národním registru osob oprávněných poskytovat platební služby[11].

Vnitrostátní identifikační číslo osoby oprávněné poskytovat platební služby: uvede se Identifikační číslo osoby (IČO).

[10] https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/index.en.html
[11] Seznamy regulovaných a registrovaných subjektů finančního trhu

Vedoucí skupiny: v případě skupin podniků podle vymezení v § 2 odst. 2 písm. j) zákona, uveďte jméno řídicího závodu.

Země dotčené incidentem: země, ve kterých má incident dopad (např. je zasaženo několik poboček oznamující osoby nacházejících se v různých zemích), bez ohledu na závažnost v jiných zemích. Nemusí se jednat o domovský členský stát.

Hlavní kontaktní osoba: jméno a příjmení osoby odpovědné za oznámení incidentu.

E-mail: e-mailová adresa, na kterou lze v případě potřeby zasílat žádosti o bližší vysvětlení. Může se jednat o osobní nebo služební e-mailovou adresu.
Telefon: telefonní číslo, na které lze zavolat s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo služební telefonní číslo.
Další kontaktní osoba: jméno a příjmení další osoby, kterou může Česká národní banka kontaktovat s dotazy týkajícími se incidentu, pokud není hlavní kontaktní osoba k dispozici.
E-mail: e-mailová adresa další kontaktní osoby, na kterou lze v případě potřeby zasílat žádosti o bližší vysvětlení. Může se jednat o osobní nebo služební e-mailovou adresu.
Telefon: telefonní číslo další kontaktní osoby, na které lze zavolat s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo služební telefonní číslo.

Oznamující subjekt: vzhledem k nemožnosti přeneseného či konsolidovaného oznamování nepřichází vyplnění tohoto oddílu v úvahu.

A 2 – Zjištění incidentu a prvotní klasifikace

Datum a čas zjištění incidentu: datum a čas, kdy byl incident poprvé identifikován.
Datum a čas klasifikace incidentu: datum a čas, kdy byl bezpečnostní nebo provozní incident klasifikován jako závažný.
Kdo incident zjistil: uveďte, zda byl incident odhalen uživatelem platební služby, někým v rámci oznamující osoby (např. funkce interního auditu) nebo externí stranou (např. externím poskytovatelem služeb). Pokud se nejedná o žádnou z uvedených možností, vysvětlete v příslušném poli.
Druh incidentu: uveďte, zda se podle vašeho nejlepšího vědomí jedná o bezpečnostní nebo provozní incident, pokud je tato informace dostupná.

Provozní: incident vyplývající z procesů, osob a systémů, které jsou nedostatečné či selhaly, nebo událostí vyšší moci, které mají dopad na integritu, dostupnost, důvěrnost a/nebo autenticitu služeb souvisejících s platbami.
Bezpečnostní: neoprávněný přístup, používání, zveřejnění, narušení, změna nebo zničení aktiv oznamující osoby s dopady na integritu, dostupnost, důvěrnost a/nebo autenticitu služeb souvisejících s platbami. K tomu může dojít mimo jiné v případě, že u oznamující osoby dojde k narušení bezpečnosti sítě nebo informačních systémů.

Kritéria vedoucí k oznámení o závažném incidentu: uveďte, která kritéria vedla k vypracování oznámení o závažném incidentu. Existuje vícero možností výběru kritérií: dotčené platební transakce, dotčení uživatelé platebních služeb, výpadek služby, narušení zabezpečení sítě nebo informačních systémů, ekonomický dopad, vysoká úroveň interní eskalace, ostatní potenciálně dotčené osoby oprávněné poskytovat platební služby nebo příslušné infrastruktury nebo reputační dopad.
Stručný a obecný popis incidentu: stručně vysvětlete nejdůležitější problémy související s incidentem, včetně možných příčin, bezprostředních dopadů atd.
Případný dopad v jiných členských státech EU: stručně vysvětlete, jaký dopad měl incident v jiném členském státě EU (např. na uživatele platebních služeb, osoby oprávněné poskytovat platební služby a/nebo platební infrastruktury). Je-li to možné, poskytněte v příslušných lhůtách pro oznamování překlad do angličtiny.
Oznamování jiným orgánům: uveďte, zda incident byl nebo bude oznámen jiným orgánům na základě samostatných rámců pro oznamování incidentů, pokud je to v době oznamování známo. Pokud ano, uveďte příslušné orgány.
Důvody pro pozdní předložení úvodního oznámení: vysvětlete důvody, proč jste ke klasifikaci incidentu potřebovali více než 24 hodin.

B – Průběžné oznámení

B 1 – Obecné údaje

Podrobnější popis incidentu: popište hlavní rysy incidentu zahrnující alespoň informace o konkrétním problému a příslušných souvislostech, dále to, jak incident začal a jak se vyvíjel, a důsledky, zejména pro uživatele platebních služeb atd. Uveďte také informace o případné komunikaci s uživateli platebních služeb.

Souvisí incident s předchozími incidenty?: uveďte, zda incident souvisí s předchozími incidenty, pokud tyto informace máte k dispozici. Pokud incident s předchozími incidenty souvisí, uveďte se kterými.
Byli dotčeni nebo zapojeni další poskytovatelé služeb či třetí strany?: Pokud tyto informace máte k dispozici, uveďte, zda se incident dotkl jiných poskytovatelů služeb či třetích stran, na které byly outsourcovány provozní funkce, nebo kteří byli nějak zapojeni do incidentu. Pokud se incident dotkl jiných poskytovatelů služeb či třetích stran, nebo do něj byli nějak zapojeni, poskytněte jejich seznam a uveďte další podrobnosti.
Bylo zahájeno krizové řízení (interní a/nebo externí)?: uveďte, zda bylo zahájeno krizové řízení (interní a/nebo externí). Pokud ano, uveďte další podrobnosti.

Datum a čas vzniku incidentu: datum a čas začátku incidentu, je-li znám.
Datum a čas, kdy u incidentu došlo nebo podle očekávání dojde k návratu do původního stavu: uveďte datum a čas, kdy incident byl nebo podle očekávání bude pod kontrolou, a kdy došlo nebo podle očekávání dojde k návratu k normálnímu provozu.
Dotčené funkční oblasti: uveďte krok nebo kroky platebního procesu, kterých se incident dotkl, jako je ověření/autorizace, komunikace, zúčtování, přímé vypořádání, nepřímé vypořádání a další.

- **Ověření/autorizace:** postupy, které osobě oprávněné poskytovat platební služby umožňují ověřit totožnost uživatele platebních služeb nebo platnost použití konkrétního platebního prostředku, včetně využití osobních bezpečnostních údajů uživatele a udělení souhlasu uživatele platebních služeb (nebo třetí strany jednající jeho jménem) k převodu peněžních prostředků.
- **Komunikace:** tok informací za účelem identifikace, ověřování, oznamování a poskytování informací mezi poskytovateli, kteří vedou platební účet, poskytovateli platební služby nepřímého dání platebního příkazu, poskytovatelem služby informování o platebním účtu, plátci, příjemci a dalšími osobami oprávněnými poskytovat platební služby.
- **Zúčtování:** proces předání, vypořádání a kontroly souladu údajů (rekonciliace) a v některých případech potvrzení převodních příkazů před vypořádáním, včetně případného započtení příkazů a stanovení konečných pozic pro vypořádání.
- **Přímé vypořádání:** dokončení platební transakce nebo zpracování, jehož cílem je splnění závazků účastníků převodem peněžních prostředků, jestliže tento úkon provádí sama dotčená oznamující osoba.
- **Nepřímé vypořádání:** dokončení platební transakce nebo zpracování, jehož cílem je splnění závazků účastníků převodem peněžních prostředků, jestliže tento úkon provádí jiná osoba oprávněná poskytovat platební služby jménem dotčené oznamující osoby.
- **Jiné:** dotčenou funkční oblastí není žádná z výše uvedených možností. Ve volném textovém poli uveďte další podrobnosti.

Změny oproti předchozím oznámením: uveďte změny oproti informacím uvedeným v předchozích oznámeních týkajících se stejného incidentu (např. v úvodním oznámení, případně v průběžném oznámení).

B 2 – Klasifikace incidentu/informace o incidentu

Dotčené transakce: Oznamující osoby by měly uvést, které prahové hodnoty byly nebo pravděpodobně budou incidentem dosaženy, a související údaje: počet dotčených platebních transakcí, procentní podíl dotčených transakcí z počtu platebních transakcí prováděných prostřednictvím stejných platebních služeb, které byly incidentem dotčeny, a celkovou hodnotu platebních transakcí. Oznamující osoby by měly uvést konkrétní hodnoty těchto proměnných, přičemž se může jednat o skutečné údaje, nebo o odhady. Oznamující osoby by obecně měly jako „dotčené transakce“ chápat veškeré vnitrostátní a přeshraniční platební transakce, které incidentem byly nebo pravděpodobně budou přímo nebo nepřímo dotčeny, a zejména pak transakce, které nebylo možné iniciovat nebo zpracovat, transakce, u kterých došlo k pozměnění obsahu platební zprávy, a transakce, k nimž byl příkaz zadán podvodně (bez ohledu na to, zda peněžní prostředky byly či nebyly získány zpět). Dále by oznamující osoby měly za běžnou úroveň platebních transakcí považovat denní roční průměr vnitrostátních a přeshraničních platebních transakcí provedených prostřednictvím stejných platebních služeb, které byly incidentem dotčeny, s použitím předchozího roku jako referenčního období pro výpočet. Jestliže oznamující osoby tento údaj nepovažují za vypovídající (např. kvůli sezónnosti), měly by místo toho použít jinou, více vypovídající metriku, a sdělit České národní bance odpovídající odůvodnění tohoto přístupu v poli „Poznámky“. Částky platebních transakcí vyjádřené v měně jiné než euro by měly oznamující osoby při výpočtu prahových hodnot a vykazování hodnoty transakcí, které byly dotčeny, převést na euro pomocí referenčního směnného kurzu ECB pro den předcházející dni předložení oznámení o incidentu.
Dotčení uživatelé platebních služeb: Oznamující osoby by měly uvést, které prahové hodnoty byly nebo pravděpodobně budou incidentem dosaženy, a související údaje: celkový počet uživatelů platebních služeb, kteří byli incidentem dotčeni, a procentní podíl dotčených uživatelů platebních služeb z celkového počtu uživatelů platebních služeb. Oznamující osoby by měly uvést konkrétní hodnoty těchto proměnných,

přičemž se může jednat o skutečné údaje, nebo o odhady. Oznamující osoby by měly jako „dotčené uživatele platebních služeb“ chápat všechny klienty (vnitrostátní nebo zahraniční, spotřebitele nebo podnikatele), kteří mají s dotčenou oznamující osobou smlouvu, na jejímž základě mají přístup k dotčené platební službě, a kteří pociťují nebo pravděpodobně pocítí důsledky incidentu. Při určování počtu uživatelů platebních služeb, kteří by bývali mohli platební službu využívat během trvání incidentu, by oznamující osoby měly použít odhady vycházející z dřívější činnosti. Dále by oznamující osoby měly jako celkový počet uživatelů platebních služeb použít souhrnný počet vnitrostátních a přeshraničních uživatelů platebních služeb, kteří jsou s nimi smluvně vázáni v okamžiku incidentu (popřípadě nejaktuálnější dostupný údaj) a mají přístup k dotčené platební službě bez ohledu na jejich velikost nebo na to, zda jsou považováni za aktivní nebo pasivní uživatele platebních služeb.

Narušení zabezpečení sítě nebo informačních systémů: Oznamující osoby by měly určit, zda nějaká škodlivá činnost neohrozila dostupnost, autenticitu, integritu nebo důvěrnost sítě nebo informačních systémů (včetně dat) souvisejících s poskytováním platebních služeb.

Délka výpadku služby: Oznamující osoby by měly uvést, zda při incidentu je nebo pravděpodobně bude dosaženo prahové hodnoty, a související údaj: celkovou délku výpadku služby. Oznamující osoby by měly uvést konkrétní hodnotu této proměnné, přičemž se může jednat o skutečný údaj, nebo o odhad. Oznamující osoby by měly zohlednit dobu, po kterou trvá nebo pravděpodobně bude trvat výpadek jakéhokoliv úkolu, procesu nebo kanálu vztahujícího se k poskytování platebních služeb, který tudíž znemožňuje i) iniciování a/nebo provedení platební služby a/nebo ii) přístup k platebnímu účtu. Oznamující osoby by měly určit délku výpadku služby od okamžiku, kdy výpadek začne, přičemž by měly zohlednit časové úseky, kdy obvykle vykonávají činnosti potřebné pro provedení platebních služeb, a v případě potřeby i dobu, kdy mají zavřeno a kdy provádějí údržbu. Nemohou-li oznamující osoby určit, kdy výpadek služby začal, měly by ve výjimečných případech určit délku výpadku služby od okamžiku, kdy byl výpadek zjištěn.

Ekonomický dopad: Oznamující osoby by měly uvést, zda při incidentu je nebo pravděpodobně bude dosaženo prahové hodnoty, a související údaj: přímé a nepřímé náklady. Oznamující osoby by měly uvést konkrétní hodnoty těchto proměnných, přičemž se může jednat o skutečné údaje, nebo o odhady. Oznamující osoby by měly zohlednit náklady přímo související s incidentem i náklady, které se k incidentu vztahují nepřímo. Oznamující osoby by měly mimo jiné vzít v úvahu ztracené peněžní prostředky nebo aktiva, náklady na výměnu hardwaru nebo softwaru, další forenzní náklady nebo náklady na nápravu škod, poplatky v důsledku nedodržení smluvních povinností, sankce, externí závazky a ušlé výnosy. Pokud jde o nepřímé náklady, oznamující osoby by měly zohlednit pouze ty, které jsou již známy nebo které velmi pravděpodobně vzniknou. Náklady v měně jiné než euro by měly oznamující osoby při výpočtu prahové hodnoty a vykazování hodnoty ekonomického dopadu převést na euro pomocí referenčního směnného kurzu ECB pro den předcházející dni předložení oznámení o incidentu.

- **Přímé náklady:** náklady (v eurech) přímo způsobené incidentem, včetně nákladů na nápravu incidentu (např. ztracené peněžní prostředky nebo aktiva, náklady na výměnu hardwaru a softwaru, poplatky z důvodu nedodržení smluvních povinností).
- **Nepřímé náklady:** náklady (v eurech) nepřímo způsobené incidentem (např. náklady na odškodnění či náhradu škody klienta, případné právní náklady).

Vysoká úroveň interní eskalace: Oznamující osoby by měly zvážit, zda v důsledku dopadu na služby související s platbami byl nebo pravděpodobně bude o incidentu informován vedoucí orgán[12], a to mimo jakýkoli postup pravidelného oznamování zaznamenaných incidentů[13], a průběžně po celou dobu trvání incidentu. Dále by oznamující osoby měly zohlednit, zda v důsledku dopadu incidentu na služby související s platbami byl nebo pravděpodobně bude vyhlášen krizový režim.

Ostatní potenciálně dotčené osoby oprávněné poskytovat platební služby nebo příslušné infrastruktury: Oznamující osoby by měly posoudit dopad incidentu na infrastruktury finančního trhu, platební schémata je podporující a další osoby oprávněné poskytovat platební služby. Oznamující osoby by měly zejména posoudit, zda se incident projevil nebo pravděpodobně projeví u jiných osob oprávněných poskytovat platební služby, zda ovlivnil nebo pravděpodobně ovlivní hladké fungování infrastruktur finančního trhu a zda ohrozil nebo pravděpodobně ohrozí řádné fungování finančního systému jako celku. Oznamující osoby by měly zohlednit různé aspekty, například to, zda je dotčená komponenta či dotčený

[12] Jak je definován v obecných pokynech orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti.

[13] V souladu s obecným pokynem 60 písm. d) obecných pokynů orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti: “*účinné plány interní komunikace včetně postupů pro oznamování incidentů a jejich předání na vyšší úroveň řízení (zahrnující i stížnosti zákazníků související s bezpečností), které zajistí:*

i) aby byly incidenty s potenciálně velkým nepříznivým dopadem na kritické systémy IKT a služby v oblasti IKT oznamovány příslušnému vrcholnému vedení a vrcholnému vedení pro IKT;

ii) aby byl v případě závažných incidentů vedoucí orgán informován ad hoc a aby byl vyrozuměn přinejmenším o dopadu, reakci a dodatečných kontrolách, které mají být stanoveny v důsledku incidentů;“.

software proprietární nebo všeobecně dostupný, zda je ohrožená síť interní nebo externí a zda oznamující osoba přestala nebo pravděpodobně přestane plnit svoje povinnosti v infrastrukturách finančního trhu, jichž je členem.

Reputační dopad: Oznamující osoby by měly zvážit úroveň viditelnosti, které incident podle jejich nejlepšího vědomí na trhu dosáhl nebo pravděpodobně dosáhne. Oznamující osoby by měly zvážit zejména pravděpodobnost, že incident bude mít negativní společenský dopad, což je dobrý ukazatel jeho potenciálního dopadu na jejich pověst. Oznamující osoby by měly vzít v úvahu, zda i) si uživatelé platebních služeb nebo jiné osoby oprávněné poskytovat platební služby stěžovaly na nepříznivý dopad incidentu; ii) incident ovlivnil viditelný proces související s platební službou, a je tedy pravděpodobné, že se mu dostane nebo se mu již dostalo mediálního pokrytí (s přihlédnutím nejen k tradičním sdělovacím prostředkům, jako jsou noviny, ale také k blogům, sociálním sítím atd.; mediální pokrytí však v tomto kontextu neznamená pouze několik negativních komentářů sledujících, ale měla by existovat věrohodná zpráva nebo významný počet negativních komentářů či upozornění); iii) došlo nebo pravděpodobně dojde k nedodržení smluvních povinností, což má za následek zveřejnění právních kroků vůči oznamující osobě; iv) nebyly dodrženy požadavky regulace, což má za následek uložení dohledových opatření nebo sankcí, které byly nebo pravděpodobně budou zveřejněny; a v) k podobnému druhu incidentu došlo již dříve.

B 3 – Popis incidentu

Druh incidentu: Bezpečnostní nebo provozní (další vysvětlení je uvedeno v příslušném poli v úvodním oznámení, tj. v části A2 výše).

Příčina incidentu: uveďte příčinu incidentu, a pokud ještě není známa, tu, která je nejpravděpodobnější. Lze vybrat více možností.

Probíhá šetření: zaškrtněte políčko, jestliže je příčina v současné době neznámá.

Škodlivá činnost: činnost úmyslně zaměřená proti osobě oprávněné poskytovat platební služby. Zahrnuje škodlivý kód, shromažďování informací, průniky, útok (distribuovaným) odmítnutím služby, úmyslnou interní činnost, úmyslné externí fyzické poškození, zabezpečení informačního obsahu, podvodná jednání atd. Více informací naleznete v části C2 tohoto formuláře.

Selhání procesu: příčinou incidentu byl chybný návrh nebo provedení platebního procesu, kontrol procesu a/nebo podpůrných procesů (např. proces změny či migrace dat, testování, konfigurace, kapacita, monitorování).

Selhání systému: příčina incidentu souvisí s nevhodným návrhem, provedením, složkami, specifikacemi, integrací nebo složitostí systémů, které podporují poskytování platebních služeb.

Lidská chyba: incident byl způsoben neúmyslnou chybou člověka, ať už v rámci provádění platby (např. nahrání chybného hromadného platebního příkazu do platebního systému), nebo v souvislosti s ním (např. neúmyslné odpojení od elektrického proudu a následné pozastavení poskytování platebních služeb).

Externí události: příčina souvisí s událostmi, nad kterými dotčená organizace nemá všeobecně přímou kontrolu (např. přírodní katastrofy, selhání poskytovatele technických služeb).

Jiné: žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Dotkl se vás incident přímo nebo nepřímo prostřednictvím poskytovatele služeb?: uveďte, zda se incident týkal přímo oznamující osoby, nebo se jí dotkl nepřímo prostřednictvím třetí strany, pokud tyto informace máte k dispozici. V případě nepřímého dopadu uveďte název poskytovatele(ů) služeb.

B 4 – Dopad incidentu

Celkový dopad: uveďte, co všechno bezpečnostní nebo provozní incident ovlivnil. Lze vybrat více možností.

Integrita: zajištění správnosti a úplnosti aktiv (včetně údajů).

Dostupnost: vlastnost služeb souvisejících s platbami spočívající v tom, že jsou plně přístupné a použitelné uživateli platebních služeb podle přijatelných úrovní předem stanovených osobou oprávněnou poskytovat platební služby.

Důvěrnost: skutečnost, že se informace nezpřístupňují ani nesdělují neoprávněným osobám, subjektům nebo pro neautorizované účely.

Autenticita: vlastnost zajišťující, že je zdroj tím, za co se vydává.

Dotčené obchodní kanály: uveďte kanál nebo kanály pro komunikaci s uživateli platebních služeb dotčené incidentem. Je možné zaškrtnout více políček.

Pobočky: provozovna (s výjimkou ústředí), která je součástí osoby oprávněné poskytovat platební služby, nemá právní subjektivitu a v níž jsou přímo vykonávány některé nebo všechny platební transakce, které jsou součástí obchodní činnosti osoby oprávněné poskytovat platební služby. Všechna místa výkonu obchodní činnosti zřízená v tomtéž členském státě osobou

oprávněnou poskytovat platební služby s ústředím v jiném členském státě by měla být považována za jedinou pobočku.

Elektronické bankovnictví: zadávání platebních příkazů či souvisejících pokynů popř. poskytování informací prostřednictvím internetu.
Telefonní bankovnictví: zadávání platebních příkazů či souvisejících pokynů, popř. poskytování informací prostřednictvím telefonu.
Mobilní bankovnictví: zadávání platebních příkazů či souvisejících pokynů popř. poskytování informací prostřednictvím zvláštní aplikace v chytrém telefonu nebo v podobném zařízení.
Bankomaty: elektromechanická zařízení, která umožňují uživatelům platebních služeb výběr hotovosti z jejich účtů a/nebo přístup k dalším službám.
Místo prodeje: fyzické prostory obchodníka, ve kterých je iniciována platební transakce.
Elektronické obchodování: platební transakce je iniciována na virtuálním místě prodeje (např. pro platby iniciované prostřednictvím internetu pomocí úhrad, platebních karet, převodu elektronických peněz mezi účty elektronických peněz).
Jiné: dotčeným obchodním kanálem není žádná z výše uvedených možností. Další podrobnosti se uvedou ve volném textovém poli.

Dotčené platební služby: uveďte platební služby, které v důsledku incidentu řádně nefungují. Je možné zaškrtnout více políček.

Vložení hotovosti na platební účet: předání hotovosti podnikatelem, který poskytuje platební služby (dále jen „poskytovatel“) za účelem jejího připsání na platební účet.
Výběry hotovosti z platebního účtu: poskytovatel obdrží od uživatele platebních služeb (dále jen „uživatel“) požadavek, aby poskytl hotovost a příslušnou částku odepsal z uživatelova platebního účtu.

Operace nutné k vedení platebního účtu: úkony, které je u platebního účtu potřeba provést za účelem jeho aktivace, zrušení a/nebo správy (např. zřízení, zablokování).

Akceptace platebních prostředků[14]: platební služba, kdy poskytovatel uzavřel s příjemcem smlouvu ohledně přijetí a zpracování platebních transakcí, jež vedou k převodům peněžních prostředků příjemci.
Úhrady: platební služba spočívající v převodu peněžních prostředků z platebního účtu plátce na platební účet příjemce na základě platebního příkazu, který dává plátce přímo svému poskytovateli.
Inkasa: platební služba spočívající v převodu peněžních prostředků z platebního účtu, k němuž dává platební příkaz příjemce na základě souhlasu, který plátce udělil příjemci, poskytovateli příjemce nebo svému poskytovateli.
Platby kartou: platební služba založená na infrastruktuře a obchodních pravidlech schémat platebních karet a používaná k provedení platební transakce pomocí karty nebo telekomunikačního, digitálního či informačně-technologického zařízení nebo softwaru, je-li jejím výsledkem transakce uskutečněná debetní nebo kreditní kartou. Karetními platebními transakcemi nejsou transakce založené na jiných druzích platebních služeb.
Vydávání platebních prostředků: platební služba spočívající ve vydání platebního prostředku poskytovatelem plátce.
Poukazování peněz: platební služba spočívající v převodu peněžních prostředků, při němž plátce ani příjemce nevyužívají platební účet u poskytovatele plátce.
Služby nepřímého dání platebního příkazu: platební služba spočívající v dání platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem odlišným od poskytovatele, který pro plátce vede daný platební účet, je-li platební příkaz dán prostřednictvím internetu.
Služby informování o platebním účtu: platební služba spočívající ve sdělování informací o platebním účtu prostřednictvím internetu poskytovatelem odlišným od poskytovatele, který vede daný platební účet.

B 5 – Zmírnění incidentu

Jaká opatření byla doposud přijata nebo jsou plánována s cílem dosáhnout obnovy po incidentu?: uveďte podrobné informace o opatřeních, která byla přijata nebo jsou plánována s cílem incident dočasně řešit.

[14] Čl. 4 odst. 44 a příloha I bod 5 nařízení EP a Rady (EU) 2015/751 o mezibankovních poplatcích za karetní platební transakce.

Došlo k aktivaci plánu kontinuity činnosti a/nebo plánu obnovy provozu po havárii?: uveďte, zda ano či ne, a pokud ano, uveďte nejdůležitější informace o tom, co se stalo (tj. kdy došlo k jejich aktivaci a v čem spočívaly).

C – Závěrečné oznámení

C 1 – Obecné údaje

Aktualizace informací z úvodního oznámení a průběžných oznámení (shrnutí): uveďte další informace o incidentu, včetně konkrétních změn oproti informacím uvedeným v průběžném oznámení. Uveďte také jakékoli další relevantní informace.

Jsou zavedena všechna původní opatření?: uveďte, zda oznamující osoba musela kdykoliv během incidentu zrušit nebo oslabit některá opatření. Pokud ano, uveďte, zda jsou všechna opatření opět zavedena, a pokud ne, vysvětlete ve volném textovém poli, která opatření nejsou opět zavedena a dobu potřebnou k jejich obnovení.

C 2 – Analýza hlavních příčin a následná opatření

Co bylo hlavní příčinou (je-li již známa)?: uveďte hlavní příčinu incidentu, a pokud ještě není známa, tu, která je nejpravděpodobnější. Lze vybrat více možností. (Pamatujte, že hlavní příčinu je třeba odlišit od dopadu incidentu.)

Škodlivá činnost: externí nebo interní činnost úmyslně zaměřená proti osobě oprávněné poskytovat platební služby. Tyto činnosti jsou rozděleny do těchto kategorií:

Škodlivý kód: např. virus, červ, trojský kůň, spyware.

Shromažďování informací: např. skenování, sniffing, sociální inženýrství.

Průniky: např. kompromitovaný privilegovaný účet, kompromitovaný neprivilegovaný účet, kompromitovaná aplikace, bot.

Útok (distribuovaným) odmítnutím služby (D/DoS): pokus znepřístupnit on-line službu tím, že dojde k jejímu zahlcení provozem z více zdrojů.

Úmyslná interní činnost: např. sabotáž, krádež.

Úmyslné externí fyzické poškození: např. sabotáž, fyzický útok na prostory či datová centra.

Zabezpečení informačního obsahu: neoprávněný přístup k informacím, neoprávněná změna informací.

Podvodná jednání: neautorizované použití zdrojů, porušení autorských práv, útok typu maškaráda, phishing.

Jiné (specifikujte): žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Selhání procesu: příčinou incidentu byl chybný návrh nebo provedení platebního procesu, kontrol procesu a/nebo podpůrných procesů (např. proces změny či migrace dat, testování, konfigurace, kapacita, monitorování). Tyto činnosti jsou rozděleny do těchto kategorií:

Nedostatečné monitorování a kontrola: např. ve vztahu k probíhajícím operacím, data vypršení platnosti certifikátů, data vypršení platnosti licencí, data vypršení platnosti aktualizací, vymezené maximální hodnoty čítače, úrovně naplnění databáze, správa uživatelských práv, princip dvojí kontroly.

Problémy s komunikací: např. mezi účastníky trhu nebo v rámci organizace.

Nesprávné operace: např. žádná výměna certifikátů, plná mezipaměť.

Nedostatečné řízení změn: např. neidentifikované chyby konfigurace, zavedení včetně aktualizací, problémy týkající se údržby, neočekávané chyby.

Nedostatečnost interních postupů a dokumentace: např. nedostatek transparentnosti, pokud jde o funkce, procesy a poruchy, neexistence dokumentace.

Problémy s obnovou: např. řízení nepředvídaných událostí, nedostatečná redundance.

Jiné (specifikujte): žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Selhání systému: příčina incidentu souvisí s nevhodným návrhem, provedením, složkami, specifikacemi, integrací nebo složitostí systémů, které podporují poskytování platebních služeb. Tato selhání jsou rozdělena do následujících kategorií:

Selhání hardwaru: selhání fyzického technologického zařízení, které spouští procesy a/nebo ukládá údaje, které oznamující osoby potřebují k výkonu činnosti

související s platbami (např. selhání pevných disků, datových center, jiné infrastruktury).

Selhání sítě: selhání telekomunikačních sítí, ať už veřejných, nebo soukromých, které umožňují výměnu dat a informací (např. přes internet) během platebního procesu.

Problémy s databází: datová struktura, která uchovává osobní údaje a údaje související s platbami potřebné k provádění platebních transakcí.

Selhání softwaru/aplikace: selhání programů, operačních systémů atd., které podporují poskytování platebních služeb osobou oprávněnou poskytovat platební služby (např. poruchy, neznámé funkce).

Fyzické poškození: např. neúmyslné poškození způsobené nevhodnými podmínkami, stavebními pracemi.

Jiné (uveďte): žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Lidská chyba: incident byl způsoben neúmyslnou chybou člověka, ať už v rámci provádění platby (např. nahrání chybného hromadného platebního příkazu do platebního systému), nebo v souvislosti s ním (např. neúmyslné odpojení od elektrického proudu a následné pozastavení poskytování platebních služeb). Tyto chyby jsou rozděleny do následujících kategorií:

Neúmyslná činnost: např. chyby, omyly, opomenutí, nedostatek zkušeností a znalostí.

Nečinnost: např. kvůli nedostatku dovedností, znalostí, zkušeností, povědomí.

Nedostatečné zdroje: např. nedostatek lidských zdrojů, zaměstnanci nejsou k dispozici.

Jiné (uveďte): žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Externí událost: příčina je spojena s událostmi, které jsou zpravidla mimo kontrolu organizace. Tyto události jsou rozděleny do následujících kategorií:

Selhání dodavatele / poskytovatele technických služeb: např. výpadek elektrického proudu, výpadek internetu, právní problémy, obchodní problémy, závislost na službách.

Vyšší moc: např. výpadek elektrického proudu, požár, přírodní příčiny, jako jsou zemětřesení, povodně, silné srážky, silný vítr.

Jiné (uveďte): žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Jiné: žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

Další relevantní informace o hlavní příčině: uveďte jakékoli další informace o hlavní příčině, včetně předběžných závěrů vyvozených z analýzy hlavních příčin.

Hlavní nápravná opatření přijatá nebo plánovaná s cílem zabránit opakování incidentu v budoucnu, pokud jsou již tato opatření známa: popište hlavní opatření, která byla přijata nebo jsou plánována s cílem zabránit opakování incidentu v budoucnu.

C 3 – Doplňující informace

Byly o incidentu informovány další osoby oprávněné poskytovat platební služby?: uveďte přehled osob oprávněných poskytovat platební služby, které byly formálně či neformálně kontaktovány s cílem informovat je o incidentu, a uveďte bližší údaje o osobách oprávněných poskytovat platební služby, které byly informovány, o poskytnutých informacích a souvisejících důvodech pro poskytnutí těchto informací.

Byly proti oznamující osobě učiněny nějaké právní kroky?: uveďte, zda do doby vyplnění závěrečného oznámení byly proti oznamující osobě v důsledku incidentu podniknuty nějaké právní kroky (např. podání žaloby u soudu nebo odebrání licence).

Posouzení účinnosti přijatých opatření: uveďte, je-li k dispozici, sebehodnocení účinnosti opatření přijatých během trvání incidentu, včetně veškerých poučení vyvozených z incidentu.

VII.
Technické náležitosti předávání oznámení České národní bance

1. Oznamující osoba oznamuje bezpečnostní a provozní incidenty České národní bance prostřednictvím internetového rozhraní České národní banky pro sběr informačních povinností regulovaných subjektů.

2. Způsob hlášení oznámení prostřednictvím internetového rozhraní České národní banky pro sběr informačních povinností regulovaných subjektů je popsán na internetových stránkách České národní banky.

VIII.
Zrušovací ustanovení a účinnost

1. Tímto úředním sdělením se zrušuje Úřední sdělení České národní banky ze dne 8. ledna 2018 k hlášení bezpečnostních a provozních incidentů.

2. Podle tohoto úředního sdělení se postupuje od 1. ledna 2022.

Viceguvernér:
Ing. Marek Mora, M.E. v. r.

Sekce regulace a mezinárodní spolupráce