Řízení incidentů v souladu se současnou legislativou

část II.

Nařízení GDPR a zákon o platebním styku

Proces řízení incidentů bezpečnosti informací je u mnoha organizací ovlivněn legislativními požadavky. Jaké požadavky mohou v případě incidentu vaši společnost ovlivnit, za jakých podmínek a jakým způsobem?

incident legislativa management GDPR zákon PSD2

Úvodem

V předchozím čísle DSM bylo nastíněno, že kromě zákona o kybernetické bezpečnosti mají vliv na proces řízení incidentů i jiné legislativní předpisy. Je tak pokryta nejen oblast fungování pro stát klíčových systémů, ale také oblast ochrany údajů běžných občanů. Tato část se tedy zaměřuje především na to, jakým způsobem ovlivní proces řízení incidentů nařízení GDPR [1] (zákon o zpracování osobních údajů [2]), zákon o platebním styku [3] a související doprovodné předpisy.

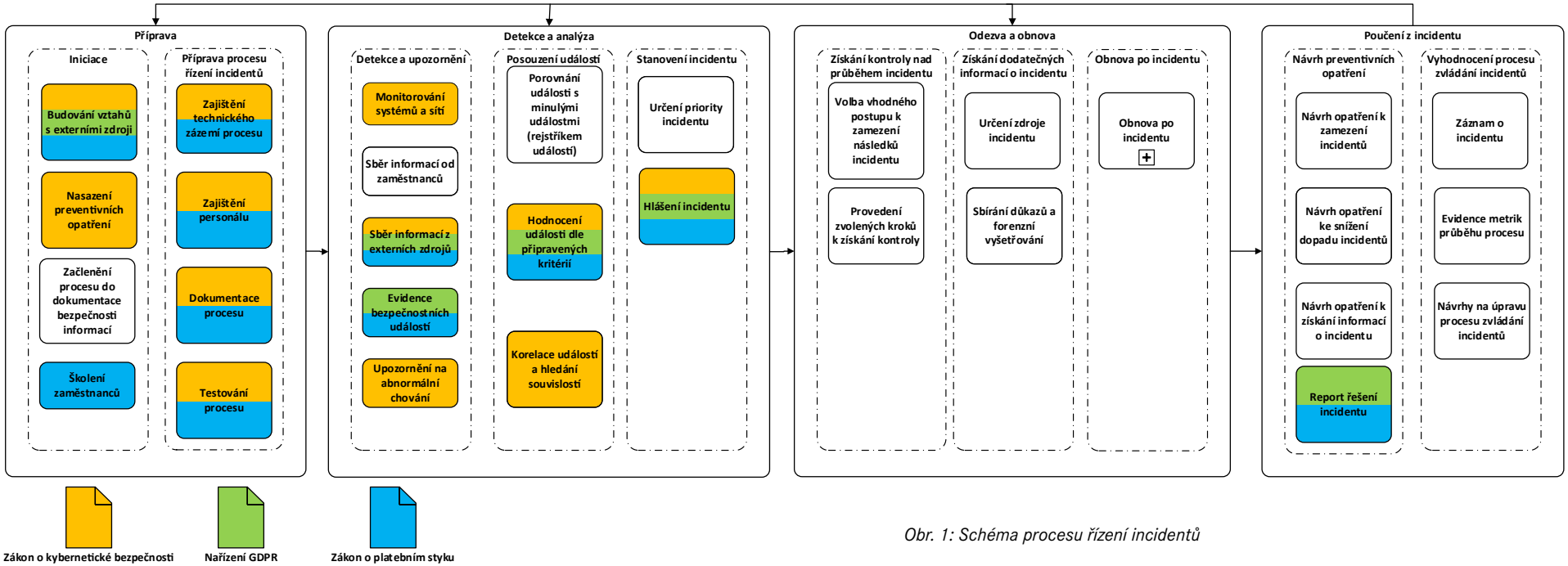
Proces řízení incidentů a jeho část

Aby bylo možné se v následujícím textu odkazovat na jednotlivé části procesu, je zde připomenuto schéma řízení incidentů z předchozího dílu.

Schéma na Obr. 1 představuje a seskupuje činnosti základních fází procesu a současně graficky znázorňuje, jaké zákony z uvedených zasahují do činností procesu.

Zákon o zpracování osobních údajů a nařízení GDPR

Legislativa v oblasti ochrany osobních údajů se zaměřuje především na ochranu práv na soukromí občanů v celé EU. Legislativa klade důraz mimo jiné na zabezpečení a transparentnost při zpracování osobních údajů a řízení incidentů lze považovat za prostředek k dosažení vhodné úrovně zabezpečení, a předpoklad pro transparentnost zpracování údajů.



Obr. 1: Schéma procesu řízení incidentů

Působnost zákona

Zákon o zpracování osobních údajů [2] (dále „zákon“), který doplňuje nařízení GDPR [1] (dále „nařízení“) se vztahuje na významný počet organizací v České republice, protože téměř každá organizace zpracovává osobní údaje. Problematika ovlivnění procesu řízení incidentů touto legislativou se vztahuje na roli správce i zpracovatele (role jsou detailněji definovány v nařízení), tedy v podstatě na všechny organizace ovlivněné touto legislativou.

Dohled nad dodržováním této legislativy zajišťuje dozorový úřad, v případě České republiky se jedná o Úřad pro ochranu osobních údajů (dále „ÚOOÚ“).

Implementační zákon neobsahuje žádné pasáže, které by měly vliv na řízení incidentů. Oblast se tak řídí jednotně pro celou EU obsahem nařízení. Existují však některá specifika, která doplňuje dozorový úřad (např. jakým způsobem se mají incidenty hlásit), a ty se mohou v jednotlivých zemích lišit.

Vliv na proces řízení incidentů

Ačkoli v nařízení nenajdeme přímou definici, že by organizace podléhající legislativě měla mít zaveden proces řízení incidentů, jsou v něm uvedeny určité požadavky, které je poměrně obtížné bez základního postupu řízení incidentů splnit. Mezi významné pasáže, ze kterých potřeba řízení incidentů plyne, řadíme recitály 85–88 a články 33 a 34.

V tomto ohledu je třeba zdůraznit, že ochrana osobních údajů i požadavky na řízení incidentů se odvíjejí od rizik, která se zpracováním osobní údajů souvisejí. Pokud organizace zpracovává údaje pouze takovým způsobem, že jakýkoli incident související se zpracováním neznamená riziko pro subjekty údajů, požadavky na proces řízení incidentů budou minimální. Mimo výše zmíněný případ je však potřebný alespoň základní proces pro řízení incidentů, jinak se organizace vystavují riziku postihu dle legislativy pro zpracování osobních údajů.

Spolupráce s dodavateli

Dle článku 28 nařízení musí správci ukotvit do smlouvy se zpracovateli (někteří dodavatelé) požadavek být nápomocen při zajišťování souladu s povinnostmi podle článků 32–36.

Jak bylo zmíněno výše, problematice incidentů se věnují články 33 a 34, a proto zpracovatel musí být nápomocen při plnění povinností identifikace a hlášení porušení zabezpečení (incidentů) osobních údajů. Z toho vyplývá konkrétní požadavek do činnosti *budování vztahů s externími zdroji*. Správce by tedy měl do smlouvy se zpracovatelem ukotvit požadavek na spolupráci v této oblasti, dohodnout vhodný kanál pro předávání informací o bezpečnostních událostech.

V souvislosti s tím je ovlivněna i činnost *sběr informací z externích zdrojů*, jelikož je třeba se se zpracovateli osobních údajů dohodnout, jaké události bezpečnosti informací budou správci hlásit. Zpracovatel totiž nemusí mít dostatek informací, aby byl schopen vyhodnotit, zda je daná událost incidentem či nikoli, zatímco správce, pokud má dostatek informací od zpracovatelů, je schopen takové posouzení provést a rozhodnout se, jaký bude další postup.

Správce by měl smluvně ukotvit i dobu pro hlášení incidentů. Dle výkladu WP29 [4] běží doba na hlášení incidentu úřadu 72 hodin od doby, kdy se o události/incidentu dozví zpracovatel. Z toho plyne, že správce musí zpracovatelům stanovit kratší dobu tak, aby stihl provést vlastní hodnocení a podat včas hlášení dozorovému úřadu. Dle našeho názoru není tento výklad správný, protože dodavatel je pouze jedním ze zdrojů, které slouží k určení toho, zda se jedná o incident či nikoliv. Tedy doba, kdy si je správce incidentu vědom nemůže být počítána od doby, kdy zpracovatel rozpoznal bezpečnostní událost, s výjimkou situace, kdy je zpracovatelem společnost poskytující služby detekce nebo řízení bezpečnostních incidentů pro správce.

Posouzení bezpečnostních událostí

Současná legislativa pro ochranu osobních údajů (články 33 a 34 nařízení) vyžaduje specifický typ hodnocení událostí bezpečnosti informací. Je třeba posoudit, zda bezpečnostní událost může znamenat pro subjekty osobních údajů riziko a jak významné. Incidenty v oblasti bezpečnosti informací bývají zpravidla hodnoceny dle rizika pro organizaci, v tomto případě se jedná o dodatečné hodnocení, nebo doplnění standardního hodnocení o hledisko subjektů. Pro hodnocení bezpečnostních událostí tímto způsobem doporučují WP29 [4] i některé dozorové úřady využít metodiku vydanou organizací ENISA [5]. Vhodným postupem je vytipovat si bezpečnostní události, které zahrnují osobní údaje, a takové události podrobit hodnocení dle uvedené nebo obdobné metodiky. Legislativa tak ovlivní činnost hodnocení *události dle připravených kritérií*.

Pro účely prokazování souladu s legislativou je vhodné si hodnocení událostí (a s ním související vstupy a výstupy) zaznamenat a evidovat, čímž je ovlivněna činnost *evidence bezpečnostních událostí*. Doporučujeme související evidenci uchovat minimálně tři roky zpětně (s ohledem na promlčecí lhůty správního řízení). Může se totiž stát, že organizace bude muset prokazovat ÚOOÚ, z jakého důvodu nebyla určitá událost v minulosti hlášena.

Hlášení incidentu

V článcích 33 a 34 nařízení je řešena problematika hlášení incidentů v případě, kdy je událost posouzena jako incident, který pravděpodobně znamená (významné) riziko pro subjekty údajů. V takovém případě je nutné provést hlášení odpovědnému dozorovému úřadu. Je tak ovlivněna činnost *hlášení incidentu*.

Odpovědným dozorovým úřadem je úřad v zemi, kde má organizace svou hlavní provozovnu (termín definován v nařízení). Odpovědný úřad definuje postup, jakým bude k hlášení incidentů docházet. V případě České republiky je postup popsán na stránkách ÚOOÚ [6]. Je zde uvedeno, co má hlášení obsahovat (není třeba uvést vše najednou, informace lze postupně doplňovat), a jak hlášení podat. Incident hlásí vždy správce.

V nařízení je stanovena lhůta, do které má k hlášení dojít – 72 hodin. Tato lhůta se týká hlášení dozorovému úřadu, z nařízení však není zcela zřejmý počátek této lhůty. Ten si dle výkladu WP29 v dokumentu [4] vykládáme jako okamžik, kdy došlo k posouzení události a bylo vyhodnoceno, že se jedná o incident, který znamená riziko pro subjekty – tedy fáze detekce a analýza (ukončení skupiny činností *posouzení události*).

Pokud incident představuje vysoké riziko pro subjekty údajů, měla by je organizace informovat. V případě, že mohou dotčené subjekty údajů provést nějaká nápravná opatření k zamezení dopadu incidentu, mělo by dojít k ohlášení co nejdříve. Způsob hlášení incidentu subjektům závisí na tom, jaké prostředky pro komunikaci se subjekty má organizace k dispozici. Informace mohu být zaslány na e-mailové adresy, předány formou telefonního hovoru nebo mohou být zveřejněny (např. na stránkách organizace či ve sdělovacích prostředcích).

Pokud je organizace v pozici zpracovatele, měla by dle článku 33 nařízení hlásit události (incidenty) správci, dle dohody (smlouvy) s ním.

Report opatření

Součástí hlášení incidentu je i popis opatření, která správce přijal nebo navrhl v reakci na daný incident, tím je požadována činnost *report řešení incidentu*.

Tato činnost navazuje na skupinu činností návrh *preventivních opatření*. U hlášení souvisejících s touto činností

již není správce vázán výše zmíněnou oznamovací lhůtou (72 hodin od detekce) a informace mohou být předány ÚOOÚ dodatečně, avšak bez zbytečného odkladu.

Shrnutí

Ukazuje se, že některé dozorové úřady plánují trestat významné nedostatky v oblasti řízení incidentů nejtvrdším způsobem (takovou informaci máme i od ÚOOÚ). Příkladem jsou navrhované pokuty britským dozorovým úřadem (ICO) 99 milionů £ pro Mariott a 183 milionů £ pro British Airways. V obou případech se jednalo o dlouhodobé nedetekované úniky osobních údajů (nedostatky ve fázi Detekce a Analýza). V případě udělení pokuty 1,5 milionu Kč společnosti Mall, a. s., za únik osobních údajů zmiňuje ÚOOÚ ve zdůvodnění výše pokuty mimo jiné i nedostatky v procesu řízení incidentů, protože únik probíhal dlouhodobě (problémy ve fázi Detekce a Analýza). Ve výše uvedených případech lze očekávat, že by udělené (navrhované) pokuty byly nižší, pokud by společnosti měly proces řízení incidentů v pořádku a dokázaly incident včas odhalit a řešit.

Zákon o platebním styku

Účelem této legislativy je mimo jiné zajistit bezpečnost platebního styku pro uživatele, a s tím souvisí i požadavek minimalizovat dopady v případě, kdy dojde k incidentu v oblasti platebního styku.

Působnost zákona

Zákon [3] (dále „zákon“) se vztahuje na omezené množství právních subjektů v České republice, které jsou zapojeny do procesu poskytování platebních služeb. Zákon implementuje do národní legislativy požadavky směrnice PSD2 [7]. Problematika hlášení incidentů se týká dle § 221 především osob oprávněných poskytovat platební služby, viz § 5 zákona pro přehled: banky, spořitelní a úvěrová družstva, instituce a vydavatelé elektronických peněz, platební instituce, správci informací o platebním účtu, a podobné. Ve všech případech je třeba mít povolení k činnosti od České národní banky, a organizace by si tak měly být vědomy situace, kdy se jich zákon týká, v takových případech ovlivňuje legislativa i jejich proces řízení incidentů.

Zákon je dále doplněn nařízením (EU) 2018/389 [8], které upřesňuje určité bezpečnostní požadavky především na systémy, které zpracovávají platební transakce (dále „nařízení“).

Dohled nad dodržováním tohoto zákona v České republice zajišťuje ČNB.

Vliv na proces řízení incidentů

V samotném zákoně je problematika incidentů uvedena jen velmi krátce, a to v § 221 zákona, kde je zmíněn požadavek na hlášení incidentů. Problematiku bezpečnostních požadavků však rozšiřují doprovodné předpisy vydané v souladu s nařízením PSD2 (článek 96 a 95) evropským orgánem pro bankovnictví (EBA): „Pokyny k bezpečnostním opatřením“ [9] a „Pokyny k oznamování významných incidentů“ [10].

Spolupráce s dodavateli

Legislativa zasahuje již do přípravné fáze, přesněji do činnosti *budování vztahů s externími zdroji*, kdy v bodu 2.8 Pokynů k bezpečnostním opatřením obsahuje požadavek na hlášení bezpečnostních událostí u dodavatelů, kteří se účastní poskytování platebních služeb.

Je tedy třeba s takovými dodavateli smluvně ukotvit spolupráci při hlášení bezpečnostních událostí a upřesnit prodlení, s jakým bude dodavatel takové informace poskytovat. To by se mělo odvíjet od činností, které pro organizaci vykonává, ale s ohledem na to, že organizace má pro hlášení incidentů poměrně krátký čas (čtyři hodiny), bude třeba i čas pro hlášení od významných dodavatelů přizpůsobit těmto požadavkům.

V souvislosti s tím je ovlivněna i činnost *sběr informací z externích zdrojů*, jelikož je třeba se s těmito dodavateli dohodnout, jaké události bezpečnosti informací budou povinným osobám hlásit.

Školení zaměstnanců

Dle bodu 8.6 Pokynů k bezpečnostním opatřením musí povinné osoby školit své zaměstnance, a to nejen

s ohledem na povědomí o bezpečnosti informací, ale také s ohledem na hlášení bezpečnostních událostí a incidentů. Je tak nutné prokazovat realizaci činnosti *školení zaměstnanců*.

Příprava procesu řízení incidentů

Skupina činností *příprava procesu řízení incidentů* je požadována dle bodu 5.5 Pokynů k bezpečnostním opatřením. Tento požadavek vede na formální realizaci činností, a to především včetně přípravy dokumentace, je tak ovlivněna skupina činností *příprava procesu řízení incidentů*.

Detekce a upozornění

V rámci činnosti *evidence bezpečnostních událostí* musí organizace dle § 31 zákona uchovávat záznamy o bezpečnostních událostech, a to po dobu pěti let.

Posouzení bezpečnostních událostí

Skupina činností *posouzení bezpečnostních událostí* je upravena legislativou, a to v Pokynech k oznamování významných incidentů v bodech 1.1–1.6. Pokyny uvádějí konkrétní metodiku hodnocení bezpečnostních událostí včetně hodnotících kritérií a prahových hodnot. Organizace tak musí uvedenou metodiku uplatnit na události, které souvisí s poskytováním platebních služeb.

Hlášení incidentů

Činnost *hlášení incidentů* je ovlivněna v návaznosti na předchozí specifické posouzení bezpečnostních událostí. Organizace, na které se vztahuje působnost zákona a související legislativy [3, 9, 10, 11], mají povinnost hlásit incidenty následovně:

- vrcholnému vedení organizace (uloženo v Pokynech k bezpečnostním opatřením bod 5.5),

- ČNB (uloženo § 221 dost. (1) zákona a v Pokynech k oznamování významných incidentů body 2.1–2.16, s tím, že vyhláška o hlášení závažných bezpečnostních a provozních incidentů [11] upřesňuje specifika tohoto procesu pro Českou republiku),
- uživateli služeb (uloženo § 221 odst. (2) zákona, ale pouze v případě může-li v důsledku incidentu vzniknout újma na jmění).

Ze specifik popsaných postupů jsou podstatné i některé další požadavky:

- je třeba hlásit pouze významné incidenty (hodnocení probíhá dle popsané metodiky výše),
- dohledový orgán je třeba informovat čtyři hodiny od zjištění incidentu,
- hlášení není jednorázové, probíhá i v následných fázích procesu (má tři části: úvodní, průběžná, závěrečná),
- hlášení probíhá prostřednictvím webové aplikace (aplikace SIPReS) na serveru ČNB,
- je možné, aby hlášení incidentů prováděla třetí strana (možnost outsourcingu v oblasti řízení incidentů).

Pokud dochází i k poskytování služeb informování o platebním účtu je v článku 35 nařízení zakotvena povinnost infor-

movat uživatele i subjekt, který jim údaje předal (tedy nejčastěji poskytovatele platebních služeb) v případě, že dojde ke ztrátě důvěrnosti „osobních bezpečnostních údajů“ (patrně údaje pro přístup – k platebním údajům či platbám).

Získání kontroly nad průběhem incidentu

Pokud došlo k nahlášení incidentu uživatelům, je třeba jej navíc informovat, jakmile pomine riziko, že by mohla vzniknout újma na jmění uživatele v důsledku incidentu, viz § 221 odst. (3). Tato činnost by měla uzavírat skupinu činností *získání kontroly nad průběhem incidentu* nebo *činnosti obnovy po incidentu*.

Report opatření

Legislativa zasahuje také do činností fáze poučení z incidentu. Dle Pokynů k bezpečnostním opatřením bod 8.2 musí být související činnosti realizovány s tím, že jejich výsledek je (dle Pokynů k oznamování významných incidentů body 2.17–2.21) obsahem závěrečné části hlášení, a tím je požadována *činnost report řešení incidentu*.

Tato činnost navazuje na činnost *sbírání důkazů a forenzní vyšetřování* a dále na skupinu činností *návrh preventivních opatření*. Činnost by měla být realizována po provedení analýzy příčin (součást činnosti *sbírání důkazů a forenzní vyšetřování*), nejpozději však dva týdny od návratu obchodní činnosti do normálního stavu (v závislosti na druhu incidentu buď ukončením skupiny činností *obnovy po incidentu*, nebo skupiny činností *získání kontroly nad incidentem*).

Shrnutí

Legislativa v oblasti platebního styku nespecifikuje mnoho technických požadavků na realizaci činností procesu řízení incidentů, chráněná data (o platebním styku) však již ze své podstaty vyžadují značný důraz na bezpečnost, jejíž nedílnou součástí je řízení incidentů. Soulad s požadavky právních předpisů v tomto případě by měl znamenat pouze drobné úpravy stávajícího procesu tak, aby byly plně v souladu s právními předpisy.

Nesplnění oznamovací povinnosti dle § 221 může být postihováno až do výše 1 milion Kč dle § 233. V krajním případě mohou organizace očekávat i odebrání licence dle § 244 odst. (1) b), pokud se přestupky opakují.

Závěrem

Předpisy zmíněné v článku nedefinují žádné protichůdné požadavky, které by působily problémy při dodržování legislativy a v zásadě legislativně ukotvují požadavky „best practice“ uvedené v normách pro oblast řízení bezpečnosti informací v organizaci a doplňují proces o určité dodatečné činnosti, které je nutné realizovat v daných situacích, především při hodnocení a hlášení bezpečnostních incidentů.

Digitální služby procházejí v posledních letech významným rozvojem, je tak nepochybně na místě legislativně zasahovat do problematiky zajištění jejich provozu a ochrany jejich uživatelů. Měla by tak být posílena odpovědnost provozovatelů a díky tomu zvýšena bezpečnost občanů, kteří tento druh služeb stále více a více využívají.

Jaromír Veber
Jaromir.Veber@aec.cz

Ing. Jaromír Veber, PhD.

Je absolventem oboru Informatika ČVUT a doktorského studia se zaměřením na bezpečnost informací na VŠE. V současnosti pracuje na pozici Security Specialist pro společnost AEC v divizi Risk & Compliance.

POUŽITÉ ZDROJE

[1] Nařízení (EU) 2016/679, *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR)*, Evropský parlament a Rada EU, 2016.
[2] Zákon č. 110/2019 Sb., *o zpracování osobních údajů*, ve znění k 24. 04. 2019.
[3] Zákon č. 370/2017 Sb., *o platebním styku*, ve znění k 01. 04. 2019.
[4] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Personal data breach notification under Regulation*. WP250rev.01. Brussels, 2018. 2016/679
[5] MANSO, Clara Galan a Sławomir GÓRNIAK, ed. *Recommendations for a methodology of the assessment of severity of personal data breaches*. Heraklion: European Union Agency for Network and Information Security, 2013. ISBN 978-92-9204-078-9.
[6] Porušení zabezpečení. *Úřad pro ochranu osobních údajů* [online]. Praha [cit. 2019-07-29]. Dostupné z: https://www.uoou.cz/poruseni%2Dzabezpeceni/ds-5020/p1=5020
[7] Směrnice (EU) 2015/2366, *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*, Evropský parlament a Rada EU, 2015.
[8] Nařízení (EU) 2018/389, *kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace*, Evropský parlament a Rada EU, 2018
[9] EBA. *Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*. Paris: European Banking Authority, 2017. EBA/GL/2017/17.
[10] EBA. *Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)*. Paris: European Banking Authority, 2017. EBA/GL/2017/10.
[11] Vyhláška č. 141/2018 Sb., *o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby*, ve znění k 01. 08. 2018.