Povinnost Národního bezpečnostního úřadu evidovat kybernetické bezpečnostní incidenty z pohledu právní úpravy ochrany osobních údajů

Základní právní rámec zajišťování kybernetické bezpečnosti

Zákon č. 181/2004 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v § 8 upravuje povinnost hlásit kybernetické bezpečnostní incidenty, ustanovení § 9 tohoto zákona potom Národnímu bezpečnostnímu úřadu ukládá vést evidenci kybernetických bezpečnostních incidentů. Tato evidence mj. obsahuje identifikační údaje systému, ve kterém se incident vyskytl, a údaje o zdroji kybernetického bezpečnostního incidentu.

Rozsah oznamovaných a Národním bezpečnostním úřadem dále evidovaných údajů bude upraven v prováděcí vyhlášce. Příslušná vyhláška dosud neprošla legislativním procesem, nicméně v jejím návrhu je tato otázka upravena v příloze 5, v dokumentu *Formulář hlášení kybernetického bezpečnostního incidentu*. Pokud tato část návrhu vyhlášky nebude změněna, pak mezi hlášenými a dále evidovanými údaji budou i informace o zdroji, ze kterého ke kybernetickému bezpečnostnímu incidentu došlo, a to v rozsahu host (jméno zařízení) nebo IP adresa, případně funkce hosta (např. server, koncové zařízení atd.)[1].

Důvodová zpráva[2] uvádí, že hlavním účelem hlášení kybernetických bezpečnostních incidentů je možnost reagovat na ně a koordinovat činnost všech dotčených orgánů. Ustanovení § 9 odst. 3 zákona o kybernetické bezpečnosti a důvodová zpráva k němu však předpokládají, že některé údaje z těchto hlášení budou předávány dalším orgánům státu pro zajištění dalších kroků, např. orgánům činným v trestním řízení pro plnění úkolů v jejich působnosti, jimiž je, zjednodušeně řečeno, vyšetřování a objasňování trestných činů.

IP adresa i údaje o jménu zařízení, které k ní bylo přiřazeno, spolu s dalšími informacemi o kybernetickém bezpečnostním incidentu, se nějakým způsobem vztahují či mohou vztahovat k fyzické osobě, která incident realizovala či se na něm jinak, i např. nevědomě, podílela. S ohledem na tuto skutečnost se jeví jako vhodné posoudit výše uvedenou povinnost Národního bezpečnostního úřadu i z pohledu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Aplikace zákona o ochraně osobních údajů - obecně

Za osobní údaje je dle § 4 písm. a) zákona o ochraně osobních údajů nutno považovat jakékoliv informace, které se vztahují k přímo či nepřímo určené nebo určitelné fyzické osobě. Nejedná se pouze o identifikační údaje, tedy údaje, ze kterých lze danou osobu ztotožnit. Pojem osobní údaje je širší a zahrnuje veškeré informace, které může správce údajů či jakákoliv další osoba, přímo či nepřímo, přiřadit ke konkrétním fyzickým osobám.

Účelem hlášení a evidence výše uvedených údajů je jejich využití při řešení kybernetických bezpečnostních incidentů, které v některých případech zjevně bude spojeno se snahou identifikovat konkrétní fyzické osoby, které se na incidentu podílely. Národní bezpečnostní úřad tak bude uchovávat, sám využívat či předávat třetím osobám (mezi nimi i orgánům

[1] Citováno dle návrhu vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), citováno dle eKLEP.

[2] Důvodová zpráva k zákonu o kybernetické bezpečnosti, zdroj: webové stránky Poslanecké sněmovny Parlamentu ČR.

činným v trestním řízení) informace vztahující se k fyzickým osobám, přičemž účelem tohoto jejich zpracování je i sledování činnosti konkrétních fyzických osob a předcházení či šetření jejich účasti na kybernetických bezpečnostních incidentech. Údaje o IP adrese, spolu s dalšími informacemi evidovanými ke konkrétnímu kybernetickému bezpečnostnímu incidentu, které jsou shromažďovány i za účelem zjištění konkrétních fyzických osob nebo jejich jednání, je tak nutno považovat za osobní údaje ve smyslu výše uvedené definice.[3,4]

Podle názoru Úřadu pro ochranu osobních údajů se tak v případě evidence a dalšího využívání hlášení o kybernetických bezpečnostních incidentech bude ze strany Národního bezpečnostního úřadu i dalších zúčastněných subjektů, které budou kybernetické bezpečnostní incidenty, resp. údaje o jejich možných původcích ve shora uvedeném rozsahu, předávat, uchovávat či využívat, jednat o zpracování osobních údajů ve smyslu zákona o ochraně osobních údajů.

Výjimky z některých zákonných povinností správce

Národní bezpečnostní úřad bude pro přijímání hlášení obsahujících dané informace, jejich evidenci a další využití, ať už samostatné nebo ve formě předání dalším subjektům, v postavení správce osobních údajů. Toto zpracování bude provádět na základě zmocnění vyplývajícího ze zvláštního právního předpisu, zákona o kybernetické bezpečnosti.

Podle názoru Úřadu pro ochranu osobních údajů je v tomto případě možné aplikovat výjimku z některých povinností uložených zákonem o ochraně osobních údajů, protože ze strany Národního bezpečnostního úřadu, pakliže bude postupovat na základě zákona a pouze v jeho mezích, se bude jednat o zpracování nezbytné pro zajištěné bezpečnosti České republiky. Takovéto zpracování osobních údajů na základě § 3 odst. 6 písm. a) zákona o ochraně osobních údajů nepodléhá povinnostem upraveným v § 5 odst. 1, § 11 a § 12 tohoto zákona. Některé další povinnosti vyplývající z tohoto zákona jsou vyloučeny na základě toho, že se jedná o zpracování osobních údajů přímo uložené zvláštním právním předpisem. Z tohoto důvodu tak na základě ustanovení § 18 odst. 1 písm. b) zákona o ochraně osobních údajů dané zpracování nepodléhá registraci u Úřadu pro ochranu osobních údajů.

Konkrétní povinnosti při zpracování osobních údajů

Výše uvedené neznamená, že zákon o ochraně osobních údajů je vyloučen jako celek. Jeho ostatní ustanovení, která nejsou dotčena ani výjimkou dle § 3 odst. 6 písm. a) zákona, ani dalšími výjimkami založenými na tom, že se jedná o zpracování údajů uložené Národnímu bezpečnostnímu úřadu zvláštním právním předpisem, je nutno respektovat. Z nich považuje Úřad pro ochranu osobních údajů za nutné upozornit především na povinnosti dle § 5 odst. 3, § 13, § 18 odst. 2 a § 27 zákona o ochraně osobních údajů.

Ustanovení § 5 odst. 3 zákona o ochraně osobních údajů ukládá správci, který provádí zpracování na základě zvláštního zákona, povinnost v maximální možné míře dbát práva na ochranu soukromého a osobního života dotčených osob. Plnění této povinnosti lze zajistit především důsledným nastavením zpracování údajů tak, aby bylo prováděno pouze v nezbytné míře vzhledem ke svému účelu, pouze po přiměřenou dobu atd. S tím

[3] K témuž závěru došla i pracovní skupina zřízení dle článku 29 Směrnice 95/46/ES, viz dokumenty č. WP 37 a WP 136. Obdobně se vyjadřuje i Soudní dvůr Evropské unie, Evropský soud pro lidská práva a část judikatury českých soudů.

[4] Nad rámec výše uvedeného je vhodné upozornit i na skutečnost, že s přechodem na novější verzi IP protokolu se zvyšuje potenciál identifikace konkrétního zařízení ve vztahu ke konkrétní osobě.

bezprostředně souvisí povinnosti správce týkající se zabezpečení zpracovávaných údajů, jež jsou blíže vymezeny v § 13 zákona o ochraně osobních údajů a které jsou standardně plněny především analyzováním daného stavu a možných rizik a přijetím a plněním relevantních bezpečnostních opatření.

Jak je již výše uvedeno, předmětné zpracování dat na základě výjimky upravené v § 18 odst. 1 písm. b) zákona o ochraně osobních údajů nepodléhá registrační povinnosti. Dle § 18 odst. 2 uvedeného zákona je však správce provádějící takovéto zpracování povinen, aby informace o zpracování v zákonem vymezeném rozsahu byly veřejně přístupné a to dálkovým přístupem nebo jinou vhodnou formou. V případě NBU tuto formu naplní prováděcí právní předpisy, které budou upravovat náležitosti a způsob hlášení bezpečnostního incidentu (§ 8 odst. 4 písm. b) zákona č. 181/2014 Sb.) a vzor oznámení kontaktních údajů (§ 16 odst. 6 téhož zákona).

Zákon o kybernetické bezpečnosti v § 9 odst. 4 NBÚ umožňuje, aby za účelem zajištění ochrany kybernetického prostoru v nezbytném rozsahu poskytoval informace z evidence incidentů mj. i orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí. Pokud by součástí poskytovaných informací byly i osobní údaje, tedy nikoliv např. statistické či jinak upravené údaje neobsahující informace využitelné k identifikaci fyzických osob či přiřaditelné k fyzickým osobám, musí být zohledněn i režim pro předávání osobních údajů do zahraničí tak, jak je upraven v § 27 zákona o ochraně osobních údajů. Stručně řečeno předávání není z pohledu tohoto zákona omezeno tehdy, pokud jsou údaje předávány do členského státu Evropské unie nebo pokud jsou osobní údaje předávány do třetích zemí na základě ratifikované a vyhlášené mezinárodní smlouvy, ze které vyplývá zákaz omezování volného pohybu osobních údajů, a nebo jestliže jsou údaje předávány na základě rozhodnutí orgánů Evropské unie. V ostatních případech předání údajů podléhá povolovacímu řízení ze strany Úřadu pro ochranu osobních údajů[5].

Závěr

Dle názoru Úřadu pro ochranu osobních údajů z dostupných legislativních podkladů vyplývá, že Národní bezpečnostní úřad bude při vedení a využívání evidence kybernetických bezpečnostních incidentů zpracovávat osobní údaje a sám bude v postavení odpovědné osoby, správce.

Některé z výše uvedených povinností, především povinnosti uložené § 5 odst. 3 a § 13 zákona o ochraně osobních údajů, lze plnit především analýzou rizik a následným nastavením vnitřních procesů tak, aby odpovídaly zákonným požadavkům. Povinnost uloženou § 18 odst. 2 zákona o ochraně osobních údajů postačí splnit tak, že, odkaz na prováděcí právní předpisy bude součástí zveřejněné informace na webových stránkách Národního bezpečnostního úřadu. V případě, kdy bude zvažováno takové předání osobních údajů do zahraničí, které podléhá povolení ze strany Úřadu pro ochranu osobních údajů, jeví se jako vhodné toto předem, před samotným formálním podnětem, s Úřadem konzultovat.

[5] http://www.uoou.cz/predavani-osobnich-udaju-do-zahranici/ds-1633/p1=1633