NÚKIB

PRŮVODCE IDENTIFIKACÍ VÝZNAMNÉHO INFORMAČNÍHO SYSTÉMU

podpůrný materiál

Verze 1.0, platná ke dni 1. 12. 2020

Obsah

Úvod

Dokument je určen všem orgánům veřejné moci jako pomocný dokument pro posouzení, zda jejich informační systémy naplní definici významného informačního systému podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“), resp. vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 360/2020 Sb. (dále jen „vyhláška o významných informačních systémech“). Tento materiál si klade za cíl proces posouzení prakticky přiblížit a odpovědět na časté dotazy, týkající se nejen identifikace významného informačního systému.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Manažerské shrnutí

Postup identifikace významného informačního systému v kostce

Proces identifikace významného informačního systému je možné zjednodušit následovně:

- Každý orgán veřejné moci vyjma obcí vytvoří seznam všech svých informačních systémů.
- U každého informačního systému jednotlivě posoudí, zda objektivně naplňuje zákonnou definici, přičemž zohlední obsah § 2 a § 3 vyhlášky o významných informačních systémech.
    - Ustanovení § 2 vyhlášky o významných informačních systémech je určeno pouze organizačním složkám státu, krajům a hlavnímu městu Praze.
    - Ustanovení § 3 vyhlášky o významných informačních systémech je určeno všem orgánům veřejné moci (uplatňují ho pro své doposud neidentifikované systémy i organizační složky státu, kraje a hlavní město Praha)
- Orgán veřejné moci začne plnit povinnosti podle zákona o kybernetické bezpečnosti.

Orgán veřejné moci

Orgán veřejné moci se vyznačuje tím, že přímo nebo zprostředkovaně autoritativně rozhoduje o právech a povinnostech jiných osob, tyto osoby nejsou s orgánem veřejné moci v rovnoprávném postavení (tzn. orgán veřejné moci vystupuje vůči dotčeným osobám vrchnostensky), a obsah rozhodnutí orgánu veřejné moci nezávisí na vůli těchto osob. Vedle toho jsou rozhodnutí orgánu veřejné moci státní mocí vynutitelná nebo může stát do takových práv a povinností zasahovat.

Výjimka pro obce

Významným informačním systémem není nikdy informační systém, jehož správcem je obec.[1] Obce tedy nemohou být správci významných informačních systémů, tedy povinné osoby podle § 3 písm. e) zákona o kybernetické bezpečnosti.

Nepřiměřené náklady

O významný informační systém podle § 3 odst. 1 vyhlášky o významných informačních systémech (nikoliv podle § 2 odst. 1 téže vyhlášky) se bude jednat pouze v případě, že naplnění dopadů uvedených v písm. a) až f) nebude možné odvrátit bez vynaložení nepřiměřených nákladů. Vynaložení nepřiměřených nákladů musí být zkoumáno a vykládáno ve světle konkrétních okolností daného případu.

[1] § 2 odst. 3 vyhlášky o významných informačních systémech

Problematika usnesení vlády č. 241 ze dne 18. dubna 2018

Toto usnesení ukládá členům vlády a vedoucímu Úřadu vlády, aby informační a komunikační technologie využívané jimi řízenými ústředními správními úřady zabezpečili podle požadavků vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti[2], alespoň na stejné úrovni, která je touto vyhláškou stanovena pro významné informační systémy.

Znění tohoto usnesení bylo následně změněno usnesením vlády č. 149 ze dne 24. února 2020, a to tak, že ukládá členům vlády a vedoucí Úřadu vlády České republiky, aby informační a komunikační technologie využívané jimi řízenými ústředními správními úřady zabezpečili podle požadavků vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, alespoň na stejné úrovni, která je touto vyhláškou stanovena pro významné informační systémy, **a to do doby nabytí účinnosti novely vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,** která je připravována podle bodu II/1. tohoto usnesení.

Tedy s nabýváním účinnosti vyhlášky o významných informačních systémech je splněna podmínka daná těmito usneseními a nadále se tato povinnost nenařizuje.

[2] Jednalo se o původní znění vyhlášky o kybernetické bezpečnosti, později byla nahrazena aktuálně účinnou vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

Vymezení pojmů

Významný informační systém

Informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.[3]

Významným informačním systémem není nikdy informační systém, jehož správcem je obec.[4] Obce tedy nemohou být správci významných informačních systémů, tedy povinnými osobami podle § 3 písm. e) zákona o kybernetické bezpečnosti.

Správce významného informačního systému

Orgán nebo osoba, které určují účel zpracování informací a podmínky provozování významného informačního systému.[5]

Správcem je ten, kdo určuje účel daného systému, respektive podmínky jeho provozování (typicky jeho vlastník), nikoliv ten, kdo se smluvně zavázal k provozu daného systému.[6]

Provozovatel významného informačního systému

Orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících významný informační systém.[7]

Pojem provozovatele informačního a komunikačního systému vyložil Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) ve speciálním podpůrném materiálu zabývajícím se výhradně tímto pojmem.[8] Z tohoto důvodu se tento průvodce tímto pojmem již dále zabývat nebude.

Identifikace významného informačního systému

Významným informačním systémem se informační systém stává okamžikem objektivního naplnění definice – neprobíhá zde žádný proces určování, ať už ze strany Úřadu, nebo ze strany daného orgánu veřejné moci. Orgány veřejné moci tedy pouze prověří, zda objektivně došlo k naplnění definice významného informačního systému, čímž významný informační systém (v případě naplnění všech definičních znaků) identifikují. Za součást této definice je však nutné považovat i kritéria obsažená ve vyhlášce o významných informačních systémech. Popis

[3] § 2 písm. d) zákona o kybernetické bezpečnosti
[4] § 2 odst. 3 vyhlášky o významných informačních systémech
[5] § 2 písm. e) zákona o kybernetické bezpečnosti
[6] Viz důvodová zpráva k zákonu o kybernetické bezpečnosti.
[7] § 2 písm. g) zákona o kybernetické bezpečnosti
[8] Podpůrný materiál „Provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, významného informačního systému nebo informačního systému základní služby podle § 2 písm. g) zákona č. 181/2014 Sb., o kybernetické bezpečnosti“, dostupný zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

procesu identifikace významného informačního systému je hlavním obsahem tohoto průvodce.

Typové významné informační systémy

Kategorie významných informačních systémů uvedené v § 2 odst. 1 vyhlášky o významných informačních systémech, u kterých se uplatňuje nevyvratitelná domněnka, že naplňují určující kritéria daná § 3 odst. 1 této vyhlášky.

ČÁST I
PROCES IDENTIFIKACE VÝZNAMNÉHO INFORMAČNÍHO SYSTÉMU

1 Obecně k identifikaci

K identifikaci významného informačního systému má být přistoupeno v okamžiku objektivního naplnění zákonné definice informačním systémem, jehož správcem je orgán veřejné moci.

> Významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Pro potřeby identifikace významného informačního systému je potřeba posoudit jednotlivé prvky této definice a zjistit, zda řešený systém v souhrnu tuto definici naplňuje.

Pro řádnou identifikaci významného informačního systému je však potřeba vycházet nikoli pouze ze zákonné definice významného informačního systému, nýbrž i z vyhlášky o významných informačních systémech, která uvedenou zákonnou definici rozvádí a v podrobnostech stanoví konkrétní podmínky, při jejichž splnění je třeba určitý systém označit za významný informační systém.[9]

Celý proces identifikace významného informačního systému je možné zjednodušeně popsat následovně:

- **Každý orgán veřejné moci vytvoří seznam všech svých informačních systémů.**
- **U každého informačního systému jednotlivě zhodnotí, zda objektivně naplňuje zákonnou definici, přičemž zohlední obsah § 2 a § 3 vyhlášky o významných informačních systémech.**
- **Začne plnit povinnosti podle zákona o kybernetické bezpečnosti.**

Jednotlivým prvkům definice se věnují následující kapitoly.

> Orgán veřejné moci může v procesu identifikace významného informačního systému využít rozhodovací schéma procesu identifikace významného informačního systému, které je přílohou tohoto průvodce.

[9] Podle § 6 písm. d) zákona o kybernetické bezpečnosti platí, že prováděcí právní předpis stanoví významné informační systémy a jejich určující kritéria.

2 Informační systém

Cílem této kapitoly je porozumět pojmu „informační systém“, tedy čím je tento pojem pro potřeby zákona o kybernetické bezpečnosti definován, co vše tento pojem tvoří a jak s tímto pojmem prakticky pracovat.

> Významným informačním systémem se rozumí **INFORMAČNÍ SYSTÉM** spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Informační systém je jako pojem v zákoně o kybernetické bezpečnosti vždy vymezen službou, pro kterou existuje.[10] V případě významných informačních systémů je to patrné především z § 2 odst. 1 vyhlášky o významných informačních systémech, který stanoví typové významné informační systémy prostřednictvím služby, kterou takový systém zajišťuje.[11] V případě posuzování naplnění určujících kritérií podle § 3 odst. 1 vyhlášky se tento přístup použije obdobně s tím rozdílem, že službu, jejíž výkon informační systém zajišťuje, orgán veřejné moci identifikuje a nadefinuje sám podle skutečného účelu posuzovaného systému a jím zajišťovaných činností.

V případě definice významného informačního systému v zákoně o kybernetické bezpečnosti není použito rozdělení na informační a komunikační systém, neboť z definice plyne, že do pojmu informačního systému spadá vždy i jeho komunikační složka.[12]

Informační systém bude vždy tvořen aktivy, tedy jak technickým a programovým vybavením a komunikačními prostředky, tak také objekty, zaměstnanci a dodavateli, stejně tak jako informacemi, které systém zpracovává a službami (procesy), které systém poskytuje.

Významný informační systém bude tedy tvořen takovými aktivy [takovým technickým a programovým vybavením, komunikačními prostředky, objekty, zaměstnanci, dodavateli,

[10] Tj. organizace si nepořizují, nevyvíjejí a neudržují systémy jen tak – systém má organizace vždy za určitým účelem, aby poskytoval organizaci určitou službu. Je tomu tak vždy, nehledě na to, zda je to služba pro interní nebo externí potřeby organizace, nebo zda byla správa systému organizaci uložena zákonem, nebo si jej organizace pořídila z vlastního rozhodnutí atd.

[11] Např. § 2 odst. 1 písm. a) vyhlášky o významných informačních systémech: *„Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný k zajištění (služby) elektronické pošty.“*

[12] Viz důvodová zpráva k zákonu o kybernetické bezpečnosti.

informacemi a službami (procesy)], která přímo podporují výkon předmětné služby v daném rozsahu a kvalitě.[13]

[13] V tomto kroku se nezohledňuje důležitost daného aktiva pro zajištění služby – všechna, i ta nejméně důležitá aktiva, jsou součástí významného informačního systému, pokud slouží k zajištění funkčnosti tohoto systému a poskytování předmětné služby v požadované kvalitě. Zohlednění důležitosti daných aktiv bude však důležitým krokem pro zavádění přiměřených bezpečnostních opatření v souladu s vyhláškou o kybernetické bezpečnosti.

3 Správa informačního systému orgánem veřejné moci

Cílem této kapitoly je porozumět pojmu „správa informačního systému“, tedy které činnosti orgánu veřejné moci jsou správou a v případě jakého vztahu k informačnímu systému jde o správu. Cílem výkladu pojmu „orgán veřejné moci“ je vymezit, které orgány a osoby naplňují tento definiční znak.

Významným informačním systémem se rozumí informační systém **SPRAVOVANÝ ORGÁNEM VEŘEJNÉ MOCI,** který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

3.1 Správa informačního systému

Správcem informačního systému je podle zákona o kybernetické bezpečnosti orgán nebo osoba, která určuje účel zpracování informací a podmínky provozování informačního systému.

Správcem informačního systému je tedy orgán nebo osoba, která určuje účel a základní způsob fungování daného systému, definuje požadavky na funkce systému a stanovuje podmínky jeho provozování. Typicky půjde o vlastníka systému, obvykle též o osobu, která zabezpečuje financování provozu daného systému. Pro určení toho, zda je určitý orgán nebo osoba správcem systému, je lhostejno, zda je systém využíván pro zajištění vlastního chodu orgánu nebo osoby, nebo pro poskytování externích služeb.

Informační systém má vždy nějakého správce a tento správce je právě jeden.[14]

V pozici správce významného informačního systému může být pouze orgán veřejné moci.

3.2 Orgán veřejné moci

Pojmem „orgán veřejné moci“ není v zákoně o kybernetické bezpečnosti výslovně definován. Přestože se jedná o neurčitý právní pojem, je jeho obsah relativně jasně dán judikaturou.[15]

Z ní pak vyplývá, že orgán veřejné moci se vyznačuje následujícími čtyřmi znaky.

---

[14] Úřad řešil v minulosti řadu případů, kdy se na něj obrátily dvě organizace tvrdící, že jsou obě správcem řešeného informačního systému. Ve všech případech došlo k definování jednoho správce tohoto systému, přičemž typickými znaky bylo vlastnění technických aktiv systému, odpovědnost za jeho provoz, finální slovo při rozhodování o změnách, nebo především jiným zákonem uložená povinnost tento systém provozovat (v tomto případě je nutné dodržovat terminologii zákona o kybernetické bezpečnosti – jiným zákonem uložená povinnost provozovat nějaký informační systém bude obsahově naplňovat typicky spíše povinnost zajistit provoz daného systému, být odpovědný za to, že systém existuje a funguje, ne jej přímo provozovat jako je tomu následně např. prostřednictvím outsourcingu u dodavatele).

[15] Detailněji je judikatura uvedena v příloze tohoto průvodce.

- **Orgán veřejné moci přímo nebo zprostředkovaně autoritativně rozhoduje o právech a povinnostech jiných osob,**
- **tyto osoby nejsou s orgánem veřejné moci v rovnoprávném postavení (tzn. orgán veřejné moci vystupuje vůči dotčeným osobám vrchnostensky),**
- **obsah rozhodnutí orgánu veřejné moci[16] nezávisí na vůli těchto osob, a**
- **tato rozhodnutí orgánu veřejné moci jsou státní mocí vynutitelná nebo může stát do takových práv a povinností zasahovat.**

Je zřejmé, že pojem orgán veřejné moci je vykládán poměrně široce a zahrnuje velké množství subjektů napříč odvětvími.

Výkon činnosti orgánu veřejné moci vždy pramení ze zákonného zmocnění.

Veřejná moc zahrnuje jak státní moc, tak veřejnou moc vykonávanou nestátními subjekty, resp. jejich orgány.[17] Orgány veřejné moci jsou proto jak státní orgány (zákonodárné, výkonné, soudní, kontrolní, dozorové – např. Poslanecká sněmovna, Senát, Prezident republiky, Vláda, ministerstva, další správní úřady, agentury, soudy, a další), tak jiné (další) orgány veřejné moci – veřejnoprávní korporace, jimiž jsou územní samosprávné celky, orgány zájmové samosprávy (stavovské komory, resp. jejich orgány), vysoké školy, zdravotní pojišťovny a další právnické a fyzické osoby, pokud vykonávají veřejnou správu.[18]

Zde je však potřeba upozornit, že výkonem veřejné moci na určitém úseku se subjekt automaticky nestává orgánem veřejné moci i ve vztahu ke všem ostatním činnostem, které vykonává. **Jako na orgán veřejné moci je na něj nahlíženo pouze ve vztahu k činnosti, která představuje výkon veřejné moci.** Pokud tentýž subjekt vykonává i jinou činnost, která nepředstavuje výkon veřejné moci (např. soukromou obchodní činnost), v této části je na něj pohlíženo jako na „běžnou“ právnickou nebo fyzickou osobu nebo veřejnoprávní korporaci, nikoli jako na orgán veřejné moci. V praxi pak tato skutečnost bude mít vliv především na určení toho, který svůj informační systém subjekt používá pro výkon veřejné moci (ve vztahu k němu pak bude subjekt orgánem veřejné moci a bude nucen zvažovat naplnění definičních znaků významného informačního systému) a který svůj informační systém používá pro výkon zbylé činnosti (tj. té, která nepředstavuje výkon veřejné moci), u něhož k naplnění definičních

[16] Pojmem rozhodování je zde myšleno rozhodování v širším slova smyslu, nikoli pouze jako proces vedoucí k vydání formalizovaného správního nebo soudního rozhodnutí.

[17] Někdy také označovanou jako *„veřejnou moc v užším slova smyslu“, „odvozenou veřejnou moc“* nebo např. *„decentralizovanou státní moc“.*

[18] Orgány veřejné moci jsou tak např. také školy, notáři, soudní exekutoři, a další. Podpůrně lze pro základní orientaci použít např. https://portal.gov.cz/obcan/rejstrik-ovm nebo https://www.czechpoint.cz/sovm/. V případě fyzické osoby jako orgánu veřejné moci je potřeba mít na paměti, že se jedná jen o ty fyzické osoby, které jsou samy orgánem veřejné moci (např. soudní exekutoři, notáři a další při výkonu své činnosti), nikoliv o ty fyzické osoby, které jsou zaměstnanci orgánu veřejné moci (např. zaměstnanci ministerstva).

znaků významného informačního systému nedojde právě pro absenci spojení s výkonem veřejné moci.

Výjimka pro obce

Přestože se v případě obcí jedná o orgány veřejné moci, a obecně by na ně vyhláška o významných informačních systémech z tohoto důvodu dopadala, je přímo v jejím textu uvedeno, že významným informačním systémem není informační systém, jehož správcem je obec. Z tohoto důvodu nebude obec, ani v přenesené, ani v samostatné působnosti, nikdy v pozici správce významného informačního systému podle § 3 písm. e) zákona o kybernetické bezpečnosti.[19]

Z tohoto důvodu nebude správcem významného informačního systému ani hlavní město Praha v případě těch informačních systémů, které spravuje výhradně v rámci výkonu působnosti obce. V případech informačních systémů, které hlavní město Praha spravuje v rámci výkonu působnosti kraje nebo tyto informační systémy využívá zároveň pro obě tyto působnosti, mohou tyto informační systémy být významnými informačními systémy.

[19] Naplnění ostatních kategorií povinných osob tím není dotčeno. V případě naplnění zákonné definice se obec dokonce může stát provozovatelem významného informačního systému a být touto povinnou osobou podle § 3 písm. e) zákona o kybernetické bezpečnosti, byť je tato situace nepravděpodobná.

4 Kritická informační infrastruktura a informační systém základní služby

Cílem této kapitoly je přiblížit problematiku situace, kdy informační systém může naplňovat různé kategorie dané zákonem o kybernetické bezpečnosti.

> Významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné moci, **KTERÝ NENÍ KRITICKOU INFORMAČNÍ INFRASTRUKTUROU ANI INFORMAČNÍM SYSTÉMEM ZÁKLADNÍ SLUŽBY** a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

V kapitole výše je definován informační systém tak, jak na něj pohlíží zákon o kybernetické bezpečnosti. V okamžiku, kdy je u takového informačního systému zvažováno, zda a jakou kategorii danou zákonem o kybernetické bezpečnosti naplní, může dojít ke zjištění, že naplňuje více kategorií, resp. že svou povahou nebo svými dopady naplňuje jak kritéria pro významný informační systém, tak pro kritickou informační infrastrukturu nebo informační systémem základní služby.[20]

V případě, že určitý informační systém je určen kritickou informační infrastrukturou nebo informačním systémem základní služby, nebude se jednat o významný informační systém (není třeba ani posuzovat naplnění definičních znaků významného informačního systému), ale bude na takový informační systém pohlíženo stále jako na kritickou informační infrastrukturu, resp. jako na informační systém základní služby.

Praktické zjištění této skutečnosti je jednoduché, neboť jak kritická informační infrastruktura, tak informační systém základní služby jsou určeny autoritativně rozhodnutím (resp. opatřením obecné povahy) Úřadu.[21] Tato rozhodnutí a opatření obecné povahy jsou správcům určovaných systémů vždy řádně doručena, orgán veřejné moci si tedy skutečnosti, že je jeho systém určen kritickou informační infrastrukturou nebo informačním systémem základní služby, musí být vědom.

[20] Například bude informační systém, který by teoreticky byl významný informační systém (např. informační systém zajišťující spisovou službu), součástí typicky většího celku, který bude informačním systémem kritické informační infrastruktury (např. informační systém zajišťující činnosti ministerstva – ten pak bude obsahovat nejen zmíněnou spisovou službu, ale i další složky).

[21] K určení kritické informační infrastruktury dochází na základě opatření obecné povahy vydaného Úřadem postupem podle § 9 odst. 3 písm. c) krizového zákona ve spojení s § 22 písm. n) zákona o kybernetické bezpečnosti, nebo na základě rozhodnutí Vlády postupem podle § 4 odst. 1 písm. e) krizového zákona. K určení informačního systému základní služby dochází na základě rozhodnutí Úřadu postupem podle § 22a zákona o kybernetické bezpečnosti.

5 Omezení nebo výrazné ohrožení výkonu působnosti orgánu veřejné moci

Cílem této kapitoly je vysvětlit a přiblížit samotný proces identifikace významného informačního systému a osvětlit obsah pojmů, které jsou ve vyhlášce o významných informačních systémech použity.

> Významným informačním systémem (se rozumí) informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby **A U KTERÉHO NARUŠENÍ BEZPEČNOSTI INFORMACÍ MŮŽE OMEZIT NEBO VÝRAZNĚ OHROZIT VÝKON PŮSOBNOSTI ORGÁNU VEŘEJNÉ MOCI.**

Poslední část zákonné definice odkazuje do vyhlášky o významných informačních systémech, když říká, že významným informačním systémem je takový informační systém, u kterého narušení důvěrnosti, integrity nebo dostupnosti informací a dat může omezit nebo výrazně ohrozit výkon těch činností, pro které je ten, kdo identifikaci významného informačního systému provádí, orgánem veřejné moci.

V souladu s § 6 písm. d) zákona o kybernetické bezpečnosti prováděcí právní předpis stanoví významné informační systémy a jejich určující kritéria. Uvedené je v kontextu zákonné definice významného informačního systému třeba chápat tak, že **vyhláška stanoví jednak významné informační systémy**, tedy systémy, u kterých je naplnění podmínky způsobilosti narušení bezpečnosti informací omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci presumováno (bez dalšího zkoumání), **jednak stanoví kritéria**, pomocí kterých bude u dalších systémů (nespadajících do první kategorie) posuzováno, zda u nich může narušení bezpečnosti informací omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Tato určující kritéria tedy budou *de facto* vykládat pojem „omezit nebo výrazně ohrozit“.[22]

Je nutné mít na paměti, že informační systém je sice významným informačním systémem z důvodu činností, které představují výkon působnosti orgánu veřejné moci, avšak nelze to pojímat tím způsobem, že významný informační systém musí k výkonu této působnosti sloužit výhradně.

V praxi budou informační systémy (např. elektronická pošta) sloužit jak k výkonu působnosti orgánu veřejné moci, tak i k takové činnosti, která výkon působnosti orgánu veřejné moci nepředstavuje (např. soukromá obchodní činnost). I v takovém případě se však bude jednat

[22] Rozhodně se tedy **nejedná** o jakousi formu „dvojstupňového“ posuzování, při kterém by mohlo dojít k situaci, kdy dojde k naplnění určujících kritérií v § 3 odst. 1 vyhlášky a poté je konstatováno, že i přesto řešený systém nemůže „*omezit nebo výrazně ohrozit*“ výkon působnosti orgánu veřejné moci, a proto nenaplňuje definici významného informačního systému.

o významný informační systém, protože tento informační systém zajišťuje výkon působnosti orgánu veřejné moci, přičemž ostatní činnosti jsou zde „navíc“.

5.1 Vyhláška o významných informačních systémech – obecně

Vyhláška o významných informačních systémech se v roce 2020 dočkala zjednodušení, které její čtení oproti původním verzím zpřehledňuje. Vyhlášku je možno pomyslně rozdělit do těchto tří částí:

1. **Seznam informačních systémů orgánu veřejné moci**[23]
2. **Typové významné informační systémy**[24]
3. **Určující kritéria pro významné informační systémy**[25]

Prvním krokem, který musí provést **každý orgán veřejné moci,** je vytvoření seznamu informačních systému, které spravuje. Po vytvoření tohoto seznamu se následný postup rozdělí podle toho, zda je orgán veřejné moci také organizační složkou státu, krajem nebo hlavním městem Praha.

Orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, zhodnotí nejdříve naplnění § 2 odst. 1 vyhlášky. **Jeho informační systémy, které jsou v § 2 odst. 1 vyhlášky uvedeny, jsou automaticky významnými informačními systémy** a orgán veřejné moci je dále nijak neposuzuje (ustanovení zakládá nevyvratitelnou právní domněnku, že se v případě těchto typových informačních systémů jedná vždy o významný informační systém). **Po zhodnocení informačních systémů podle § 2 odst. 1 vyhlášky tento orgán veřejné moci posoudí všechny své zbývající informační systémy podle § 3 odst. 1 této vyhlášky** (podkapitoly 5.3 a 5.4 tohoto průvodce)**.**

Orgány veřejné moci, které nejsou organizačními složkami státu, kraji nebo hlavním městem Praha, posoudí všechny své informační systémy rovnou podle § 3 odst. 1 vyhlášky (podkapitola 5.4 tohoto průvodce)**.** Ustanovení § 2 odst. 1 vyhlášky se na ně nevztahuje.

5.2 Seznam informačních systémů orgánu veřejné moci

Před samotným procesem identifikace významných informačních systémů u konkrétního orgánu veřejné moci je potřeba získat přehled o všech informačních systémech, které tento orgán při své činnosti využívá, a u kterých tedy bude posuzováno naplnění definičních znaků významného informačního systému. Za tím účelem vyhláška stanoví, že **každý orgán veřejné moci vede seznam všech informačních systémů, kterých je správcem.**

[23] § 3 odst. 2 vyhlášky o významných informačních systémech
[24] § 2 odst. 1 vyhlášky o významných informačních systémech
[25] § 3 odst. 1 vyhlášky o významných informačních systémech

Vyhláška o významných informačních systémech nepředepisuje formát, vzhled, ani bližší obsahové náležitosti takového seznamu, s výjimkou toho, že součástí seznamu je písemný záznam o výsledku posouzení naplnění určujících kritérií u informačního systému, který není uveden v § 2 odst. 1 vyhlášky. I přesto je však pro větší přínosnost seznamu možné doporučit, aby obsahoval minimálně následující části.

1. **Označení informačního systému**

Pojmenování řešeného informačního systému.

2. **Označení výkonu působnosti, který systém podporuje**

Protože je definičním znakem významného informačního systému skutečnost, že narušení jeho bezpečnosti může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci, je vhodné v rámci seznamu uvést, pro výkon jaké působnosti (jaké činnosti orgánu veřejné moci) byl zvažován při posuzování daných kritérií.[26]

3. **Informaci, zda jde o významný informační systém nebo ne**

Údaj o tom, zda na základě posouzení naplnění zákonné definice došlo k identifikaci informačního systému jako významného informačního systému, nebo ne.

4. **Na základě jakých kritérií se jedná o významný informační systém**

Údaj o tom, na základě jakého ustanovení vyhlášky je daný informační systém považován za významný informační systém. **Jde tedy o výslovný odkaz na konkrétní písmeno v rámci § 2 odst. 1 nebo § 3 odst. 1 vyhlášky o významných informačních systémech.** V případě, že informační systém nenaplňuje žádná z výše uvedených ustanovení a není tedy významným informačním systémem, není zde co vyplňovat.

5. **Důvod toho, proč k naplnění definice významného informačního systému dochází nebo nedochází**

Krátký popis důvodů, pro které dochází k naplnění nebo nenaplnění definice významného informačního systému. Zde je prostor k popisu nejhoršího možného dopadu z pohledu dostupnosti, důvěrnosti i integrity, a to především v případě, že by informační systém žádné z určujících kritérií neměl naplnit. Stejně tak je na tomto místě prostor pro to uvést například informaci o tom, že informační systém není významným informačním systémem z toho důvodu, že je již součástí určené kritické informační infrastruktury nebo informačního systému základní služby. Vhodné je uvést též jakékoli další relevantní informace či komentáře upřesňující nebo doplňující seznam informačních systémů.

[26] Konkrétní působnosti budou jistě jak obecné (např. vedení správního řízení podle správního řádu), tak mohou být i uvedeny specificky [např. určování provozovatele základní služby a informačního systému základní služby podle § 22 písm. p) zákona o kybernetické bezpečnosti].

6. Další doplňující informace

Vedle výše uvedených náležitostí by měl seznam obsahovat také základní informace identifikující dokument jako takový, verzi dokumentu, datum poslední změny, informaci o tom, kdo seznam vytvořil, informaci o tom, kdo a kdy dokument schválil (stejně jako jeho podpis), pořadové číslo informačního systému pro lepší orientaci, celkový počet stran, pokud je seznam vícestránkový, informaci o způsobu nakládání s tímto seznamem (např. prostřednictvím tzv. TLP protokolu[27]) atd.

Informace o tom, zda se v případě konkrétního řešeného informačního systému jedná o významný informační systém, na základě jakých kritérií a z jakého důvodu – případně informace o tom, že se o významný informační systém nejedná, že nebyla naplněna žádná kritéria a důvod – **lze společně považovat za písemný záznam o výsledku posouzení naplnění určujících kritérií u informačního systému dle § 3 odst. 2 vyhlášky.** V případě významných informačních systémů podle § 2 odst. 1 vyhlášky je možné uvést pouze, že se v případě konkrétního řešeného informačního systému jedná o významný informační systém podle příslušného písmene § 2 odst. 1 vyhlášky – odůvodnění již není potřeba, platí zde nevyvratitelná domněnka, že se o významný informační systém jedná.[28]

> Vzor doporučeného vzhledu a obsahu seznamu informačních systémů, kterých je orgán veřejné moci správcem, je uveden v příloze tohoto průvodce.

5.3 Typové významné informační systémy (§ 2 odst. 1 vyhlášky)

Pokud je orgán veřejné moci zároveň organizační složkou státu, krajem nebo hlavním městem Praha, nesmí jeho pozornosti uniknout § 2 odst. 1 vyhlášky o významných informačních systémech. **Toto ustanovení vymezuje tzv. typové významné informační systémy.**

Jedná se o obecně vymezené informační systémy, které, pokud budou spravovány organizační složkou státu, krajem nebo hlavním městem Praha, nebudou kritickou informační infrastrukturou ani informačními systémy základní služby a budou využívány pro výkon veřejné moci v působnosti této **organizační složky státu, kraje nebo hlavního města Praha, budou vždy významnými informačními systémy.**

U typových významných informačních systémů se dále nezkoumá naplnění kritérií podle § 3 odst. 1 vyhlášky o významných informačních systémech, pro jejich identifikaci a podřazení pod zákon o kybernetické bezpečnosti postačí prosté naplnění § 2 odst. 1.

---

[27] Dostupný zde: https://www.first.org/tlp/

[28] Důvodová zpráva k novele vyhlášky o významných informačních systémech: *„V § 2 odst. 4 je uvedena nevyvratitelná domněnka, podle které platí, že významné informační systémy uvedené v odstavci 1 naplňují určující kritéria.“*

Před přiblížením jednotlivých typových významných informačních systémů je potřeba upozornit na jedno specifikum spojené se zněním § 2 odst. 1 vyhlášky – s ohledem na potřebu vyvolanou v rámci legislativního procesu při vzniku novely této vyhlášky došlo k rozčlenění § 2 odst. 1 do tří částí a stanovení postupné účinnosti těchto jednotlivých částí. V průběhu tedy § 2 odst. 1 vyhlášky o významných informačních systémech změní svůj obsah následovně:

V období od 1. ledna 2021 do 31. prosince 2021

Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci, nebo
b) kontrolní nebo inspekční činnosti anebo státního dozoru.

V období od 1. ledna 2022 do 31. prosince 2022

Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
b) kontrolní nebo inspekční činnosti anebo státního dozoru,
c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,
d) výkonu spisové služby, nebo
e) vedení úřední desky způsobem umožňujícím dálkový přístup.

V období od 1. ledna 2023 dále

Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
b) kontrolní nebo inspekční činnosti anebo státního dozoru,
c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,
d) výkonu spisové služby,
e) vedení úřední desky způsobem umožňujícím dálkový přístup,
f) mezinárodní spolupráce, nebo
g) zadávání veřejných zakázek.

Při pohledu na seznam typových významných informačních systémů v jeho úplném znění (k 1. lednu 2023) je patrné, že tyto typové systémy lze s jistým zjednodušením rozdělit na ty, které se budou u organizační složky státu, kraje nebo hlavního města Prahy vyskytovat vždy (jimi budou elektronická pošta, spisová služba a úřední deska vedená způsobem umožňující dálkový přístup), a na ty typové systémy, které mohou sloužit pro určité činnosti, jež jsou v mnoha případech vykonávány prostřednictvím spisové služby (informační systém využívaný k zajištění kontrolní nebo inspekční činnosti anebo státního dozoru, výkonu veřejné moci při přípravě na krizové situace a jejich řešení, mezinárodní spolupráce nebo zadávání veřejných zakázek).

Přijímání finálního znění § 2 odst. 1 vyhlášky a rozčlenění typových systémů do jednotlivých fází účinnosti tohoto ustanovení bylo vedeno snahou o rozložení finanční zátěže spojené se zabezpečováním těch informačních systémů, které se budou vyskytovat prakticky u všech organizačních složek státu, krajů a hlavního města Prahy, do delšího časového úseku.[29] Právě z toho důvodu je proces identifikace a zabezpečování informačních systémů elektronické pošty, informačních systémů spisové služby a informačních systémů úřední desky rozložen do různých období účinnosti § 2 odst. 1 vyhlášky. K identifikaci a zabezpečování zbylých kategorií typových systémů je pak potřeba přistupovat tak, že o takové typové systémy se bude jednat pouze v případě, pokud **uvedená činnost bude vykonávána (vedle spisové služby) pomocí jiného samostatného informačního systému nebo více systémů**. Při výkladu těchto specifických pojmů je tak jejich obsah nutno posuzovat právě optikou jejich vazby k těmto samostatným systémům a vymezit je vůči spisové službě (viz dále).

Současně je třeba mít na paměti, že obsah § 2 odst. 1 vyhlášky a naplnění kritérií v něm obsažených je potřeba posuzovat vždy s ohledem na aktuální znění a obsah tohoto ustanovení. Postup organizačních složek státu, krajů a hlavního města Prahy lze demonstrovat na následujících příkladech.

Příklad 1: Orgán veřejné moci, který je zároveň organizační složkou státu, spravuje samostatný informační systém využívaný k zajištění své dozorové a kontrolní činnosti. Tento systém je nezávislý na systému spisové služby a je od něj technicky i funkčně oddělen. Tento informační systém využívaný k zajištění své dozorové a kontrolní činnosti se s účinností od 1. ledna 2021 stane významným informačním systémem podle písmena b) § 2 odst. 1 vyhlášky.

Příklad 2: Orgán veřejné moci, který je zároveň organizační složkou státu, používá pro zajištění své dozorové a kontrolní činnosti, stejně jako pro výkon dalších činností, jím spravovaný

[29] Úřad i Ministerstvo vnitra jako spolupředkladatel novely vyhlášky o významných informačních systémech si jsou vědomy toho, že zabezpečení tří základních a pro činnost orgánu veřejné moci prakticky stěžejních systémů je v případě, že tyto systémy doposud nenaplňovaly kritéria daná původním zněním vyhlášky o významných informačních systémech, finančně i časově náročná záležitost, kterou je obtížné zvládnout v požadované kvalitě za období jednoho roku (k čemuž by byly organizační složky státu, kraje a hlavního města Praha povinny, pokud by byly tyto tři systémy zahrnuty do stejné fáze účinnosti § 2 odst. 1 vyhlášky).

informační systém spisové služby. Tento orgán veřejné moci žádný jiný samostatný informační systém zajišťující výkon dozorových a kontrolních oprávnění nevyužívá a nespravuje. Tento orgán veřejné moci tedy nedisponuje informačním systémem, který by spadl do první fáze účinnosti § 2 odst. 1 vyhlášky. Na informační systém spisové služby, který současně slouží k zajištění výkonu dozorové a kontrolní činnosti, dopadne až písmeno d) § 2 odst. 1 vyhlášky účinné od 1. ledna 2022.

Příklad 3: Orgán veřejné moci, který je zároveň organizační složkou státu, vykonává svou dozorovou a kontrolní činnost pomocí tří jím spravovaných samostatných systémů. Prvním z nich je samostatný systém určený pouze pro výkon kontroly a dozoru. Druhým z nich je informační systém spisové služby. Třetím z nich je informační systém, který slouží současně pro výkon kontroly a dozoru a pro vedení úřední desky (tj. zde budou výsledky kontrolní a dozorové činnosti orgánu veřejné moci uveřejňovány). První systém bude identifikován jako významný informační systém k 1. lednu 2021 podle písmena b) § 2 odst. 1 vyhlášky. Druhý systém (spisová služba) bude identifikován jako významný informační systém nejpozději k 1. lednu 2022, a to podle písmena d) § 2 odst. 1 vyhlášky. Třetí systém (úřední deska) bude také identifikován jako významný informační systém nejpozději k 1. lednu 2022, a to podle písmena e) § 2 odst. 1 vyhlášky.

Příklad 4: Orgán veřejné moci, který je zároveň organizační složkou státu, používá pro zadávání veřejných zakázek dva jím spravované informační systémy. Prvním z nich je samostatný systém určený pouze pro zadávání veřejných zakázek. Druhým systémem je informační systém spisové služby. Zatímco první systém bude možné identifikovat jako významný informační systém až k 1. lednu 2023, a to podle písmena g) § 2 odst. 1 vyhlášky, druhý systém (spisová služba) bude identifikován jako významný informační systém nejpozději k 1. lednu 2022, a to podle písm. d) § 2 odst. 1 vyhlášky.

5.3.1 Korelace § 2 odst. 1 a § 3 odst. 1 vyhlášky o kybernetické bezpečnosti

Posouzením naplnění podmínek obsažených v § 2 odst. 1 vyhlášky o kybernetické bezpečnosti však práce orgánu veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, nekončí, neboť **ve vztahu k informačním systémům, které nenaplní kritéria uvedená v příslušném účinném znění § 2 odst. 1 vyhlášky, je tento orgán veřejné moci stále povinen posoudit naplnění určujících kritérií podle § 3 odst. 1 vyhlášky**.

Situaci lze demonstrovat na následujícím příkladu:

Pokud bude orgán veřejné moci, který je zároveň organizační složkou státu, posuzovat k 1. lednu 2021 všechny své informační systémy a mezi nimi např. samostatný informační systém využívaný k zajištění přípravy na krizové situace (nejedná se tedy o spisovou službu, ale o samostatný informační systém), zkontroluje nejdříve, zda tento systém není uveden v § 2 odst. 1 vyhlášky o významných informačních systémech. Takový systém v § 2 odst. 1 uveden není [jako typový významný informační systém se v rámci písm. c) zařadí až k 1. lednu 2022].

Organizační složka státu k němu tedy bude přistupovat jako ke každému jinému informačnímu systému a posoudí jej v souladu s § 3 odst. 1 vyhlášky (viz podkapitola 5.4).

V případě, že výsledkem posouzení bude kladné naplnění kritérií podle § 3 odst. 1 vyhlášky, bude se jednat o významný informační systém a jako takový bude veden a bude k němu tak přistupováno. Změna spojená se změnou obsahu § 2 odst. 1 vyhlášky dne 1. ledna 2022 [tedy přidání § 2 odst. 1 písm. c) „(informační systém využívaný k zajištění) *výkonu veřejné moci při přípravě na krizové situace a jejich řešení*"] pak na statusu takového systému jako významného informačního systému nic nezmění (např. nedojde k vlivu na běh lhůty podle § 31 zákona o kybernetické bezpečnosti), jen čistě pro úplnost by však mělo dojít k úpravě informací u tohoto informačního systému – významným informačním systémem nebude z důvodu naplnění některého z kritérií podle § 3 odst. 1 vyhlášky, ale z důvodu naplnění § 2 odst. 1 písm. c) vyhlášky.

V případě, že výsledkem posouzení nebude naplnění kritérií podle § 3 odst. 1 vyhlášky, nebude se v průběhu roku 2021 jednat o významný informační systém (výsledek tohoto posouzení se opět uvede v seznamu informačních systémů)**.** Změna spojená se změnou obsahu § 2 odst. 1 vyhlášky dne 1. ledna 2022 [tedy přidání § 2 odst. 1 písm. c) „(informační systém využívaný k zajištění) *výkonu veřejné moci při přípravě na krizové situace a jejich řešení*"] pak ovšem změní status tohoto informačního systému a ten se stane významným informačním systémem z důvodu naplnění § 2 odst. 1 písm. c) vyhlášky (od 1. ledna 2022 také začnou běžet lhůty dané § 31 zákona o kybernetické bezpečnosti).

Tento model se samozřejmě použije i na všechny ostatní informační systémy.

5.3.2 Organizační složka státu, kraj a hlavní město Praha

Organizačními složkami státu jsou v souladu s definicí danou zákonem č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích:

1. **Ministerstva a jiné správní úřady státu, Ústavní soud, soudy, státní zastupitelství, Nejvyšší kontrolní úřad, Kancelář prezidenta republiky, Úřad vlády České republiky, Kancelář Veřejného ochránce práv, Akademie věd České republiky, Grantová agentura České republiky.**
2. **Složky zřízené příslušným ministerstvem po předchozím souhlasu Ministerstva financí podle § 4 odst. 1 zákona o majetku České republiky a jejím vystupování v právních vztazích.**
3. **Jiná zařízení v souladu s § 51 zákona o majetku České republiky a jejím vystupování v právních vztazích.**

4. Jiná zařízení, o kterých to stanoví zvláštní právní předpis.[30]

Specificky pak zákon o majetku České republiky a jejím vystupování v právních vztazích stanoví, že Kancelář Poslanecké sněmovny a Kancelář Senátu nabývají *„obdobné postavení jako organizační složka státu“* – z tohoto důvodu však nejsou organizačními složkami státu jako takovými.

Je potřeba nezaměňovat pojem organizační složka státu s pojmy jako státní příspěvková organizace, státní podnik nebo např. veřejná výzkumná instituce. Tyto sice mohou mít s organizačními složkami státu jisté podobné rysy, nejedná se však o totožné instituty (především proto, že na rozdíl od organizačních složek státu, které vystupují v pozici vnitřních útvarů státu, mají tyto jiné typy osob právní subjektivitu).

Kraji jsou v souladu s definicí danou zákonem č. 129/2000 Sb., o krajích, veřejnoprávní korporace, které jsou územním společenstvím občanů, které má právo na samosprávu, a které mají vlastní majetek, vlastní příjmy vymezené zákonem a hospodaří za podmínek stanovených zákonem podle vlastního rozpočtu.

V České republice je na základě ústavního zákona č. 347/1997 Sb., o vytvoření vyšších územních samosprávných celků, vytvořeno celkem čtrnáct krajů.

Hlavní město Praha je v souladu s definicí danou zákonem č. 131/2000 Sb., o hlavním městě Praze, veřejnoprávní korporace, která má vlastní majetek, má vlastní příjmy vymezené zákonem a hospodaří za podmínek stanovených zákonem podle vlastního rozpočtu. Podle tohoto zákona hlavní město Praha může vystupovat jako hlavní město České republiky, kraj nebo obec. Zde je potřeba mít na paměti ustanovení § 2 odst. 3 vyhlášky o významných informačních systémech, který stanovuje, že *„významným informačním systémem není informační systém, jehož správcem je obec“*. Z tohoto důvodu bude pro praktickou aplikaci tohoto ustanovení potřeba pohlížet na slovní spojení *„a hlavní město Praha“* v § 2 odst. 1 vyhlášky jako na hlavní město Praha v pozici kraje jako správce informačního systému. Pokud tedy hlavní město Praha vykonává ať už samostatnou nebo přenesenou působnost jako kraj, budou informační systémy, které tuto krajskou působnost zajišťují, spadat pod § 2 odst. 1 vyhlášky. V rámci filozofie vyhlášky tedy nedochází ke změně oproti jejímu předchozímu znění. V případě hlavního města Prahy se dá předpokládat, že větší množství informačních systémů bude zároveň zajišťovat jak působnosti obce, tak kraje. Takové informační systémy pak budou spadat pod vymezení v § 2 odst. 1 vyhlášky, neboť (mj.) zajišťují výkon působnosti hlavního města Prahy jako kraje (jejich podpora pro činnosti obce je zde „navíc“).

[30] Podpůrně lze pro základní orientaci použít např. https://portal.gov.cz/obcan/rejstrik-ovm/kategorie/KO191/.

5.3.3 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění elektronické pošty

Elektronická pošta (e-mail) je v praxi využívána nejen pro komunikaci uvnitř správního orgánu, ale též pro komunikaci se třetími osobami v rámci působnosti orgánu veřejné moci, resp. působnosti organizační složky státu, kraje nebo hlavního města Praha.

Důvodem pro její zařazení mezi typové významné informační systémy je vedle její vysoké důležitosti pro denní praxi i to, že správní orgán je obecně vázán § 37 odst. 4 zákona č. 500/2004 Sb., správní řád (dále jen „správní řád“), podle kterého je podání vůči správnímu orgánu možné učinit písemně nebo ústně do protokolu anebo v elektronické podobě. V souladu s předpisy upravujícími vedení spisové agendy jsou správní orgány obecně povinny vykonávat svou spisovou službu v elektronické podobě a za účelem přijímání a odesílání dokumentů mít zřízenu podatelnu. S ohledem na vývoj relevantní právní úpravy[31] **je však třeba konstatovat, že veřejnosti není zapovězeno komunikovat s orgány veřejné moci i mimo podatelnu[32]**, např. na e-mailové adrese odlišné od elektronické adresy podatelny, a řádně zde doručovat úřední dokumenty. Tento závěr je mj. potvrzen i závěry Odboru legislativy a koordinace předpisů Ministerstva vnitra obsaženými v materiálu Vyřizování elektronických podání, podnětů a jiných písemností podle správního řádu s důrazem na vyřizování úkonů bez uznávaného elektronického podpisu.[33] Platí pak, že v případě, že je podání doručeno na jinou elektronickou adresu než elektronickou adresu podatelny, musí orgán sám zajistit jeho bezodkladné předání podatelně.[34] Je potřeba mít na paměti, že tato situace se může v zásadě vyskytnout u jakékoliv e-mailové adresy jakéhokoliv zaměstnance organizační složky státu, kraje nebo hlavního města Praha, a proto je nutno

[31] Do 30. června 2012 platila zákonná povinnost orgánů veřejné moci přijímat a odesílat datové právy prostřednictvím elektronické podatelny (srov. § 11 odst. 4 zákona č. 227/2000 Sb., o elektronickém podpisu, ve znění účinném do 30. 6. 2012) a současně vyhláška č. 496/2004 Sb., o elektronických podatelnách, stanovovala, že přijatá datová zpráva je považována za doručenou orgánu veřejné moci, pokud je dostupná elektronické podatelně provozované podle zvláštního právního předpisu. Tato ustanovení obou předpisů byla s účinností k 1. červenci 2012 zrušena, v současné době je tedy rozhodné především znění správního řádu a vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, která sice ve větě první § 2 odst. 1 stanoví, že veřejnoprávní původce přijímá doručené dokumenty v podatelně, nicméně hned vzápětí hovoří o situaci, kdy je dokument orgánu doručen mimo podatelnu. Právní úprava tedy s doručováním mimo podatelnu výslovně počítá. Uvedená regulace vyhlášky přitom vychází z praxe a navazuje právě na to, že jsou činěna podání i mimo podatelnu (viz důvodová zpráva k vyhlášce). Právní předpis tak zobrazuje úmysl zákonodárce posílit roli elektronické pošty jako takové a posílit principy dobré správy.

[32] S výjimkou situací, kde zákon výslovně vyžaduje doručení podání na adresu elektronické podatelny nebo prostřednictvím určeného technického zařízení (srov. např. § 14 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, nebo § 73 odst. 2 zákona č. 280/2009 Sb., daňový řád).

[33] Dostupný zde: https://www.mvcr.cz/webpm/clanek/spravni-rad-metodicke-pomucky-ke-spravnimu-radu-metodicke-pomucky-ke-spravnimu-radu.aspx.

[34] K podatelně je pak nutno uvést, že podatelna jako taková je součástí spisové služby, kterou návrh vyhlášky považuje za významný informační systém, nicméně další elektronická pošta součástí spisové služby být nemusí.

vycházet z předpokladu, že v zásadě jakákoliv e-mailová adresa orgánu veřejné moci může sloužit v tomto duchu k výkonu působnosti orgánu veřejné moci.

Zde lze odkázat i na závěry Ústavního soudu obsažené v nálezu ze dne 6. června 2007, sp. zn. I. ÚS 750/06, který potvrzuje, že „*[j]estliže zákon účastníku řízení dává možnost, aby procesní úkony činil prostřednictvím veřejné datové sítě […], pak není materiálně myslitelné, aby případné poruchy uvnitř tohoto doručovacího mechanizmu šly na jeho vrub*“. **Pro řádné fungování organizační složky státu, kraje nebo hlavního města Praha je tedy odpovídající zajištění fungování elektronické pošty, a tedy i její kybernetická bezpečnost, nezbytné.**

Kromě oficiálních procesních postupů, vyplývajících ze zákona, lze upozornit i na to, že mnohdy je elektronická pošta využívána i v rámci realizace principu dobré správy. Např. Úřad práce na svých internetových stránkách uvádí: „*E-mail bez elektronického podpisu […] můžete poslat přímo na e-mailovou adresu zaměstnance ÚP ČR, který se danou agendou zabývá. E-mail nebude považován za elektronicky podaný dokument, avšak naši zaměstnanci se budou snažit na něj odpovědět.*“[35] Externí komunikaci s občany připouští i Úřad pro ochranu osobních údajů: „*Datové zprávy zaslané orgánům veřejné moci, jejichž náležitosti neupravuje právní předpis, nemusí být podepsány zaručeným elektronickým podpisem. Jedná se například o běžnou e-mailovou komunikaci mezi pracovníky orgánu a občany*“.[36] Obdobně též Státní zemědělská a potravinářská inspekce: „*SZPI akceptuje elektronická podání zaslaná i na kontaktní adresy jednotlivých zaměstnanců SZPI, v případě, že jsou dodrženy technické a legislativní podmínky zde uvedené. Na elektronická podání zaslaná na jinou adresu než oficiální e-mailové adresy jednotlivých inspektorátů nezasílá SZPI potvrzení o doručení*.“[37] Lze předpokládat, že uvedené principy jsou přítomny u množství dalších orgánů veřejné moci a budou posilovány a rozšiřovány.

Kromě zákonem aprobovaného způsobu realizace správního podání nese elektronická pošta i další neopomenutelné prvky fungování orgánu veřejné moci, a to realizaci interních procesů souvisejících s výkonem jeho působnosti. Tyto interní procesy mohou nést důležité informace nebo osobní údaje a i přesto, že nejsou zachyceny podatelnou či spisovou službou, jsou pro fungování orgánu nepostradatelné. Aspekt ochrany elektronické pošty tak není myšlen pouze jako ochrana externí komunikace, ale i té interní, která mnohdy nese větší množství informací než samotný spis ke konkrétní věci.

Je však nutno podotknout, že v případě, kdy elektronická pošta není v žádném ohledu využívána v rámci vrchnostenského postavení organizační složky státu, kraje nebo hlavního města Praha, o významný informační systém se nejedná.

---

[35] Dostupný zde: https://portal.mpsv.cz/sz/obecne/koninf/el_zadosti
[36] Dostupný zde: https://www.uoou.cz/elektronicka-podatelna/os-1007/p1=3109
[37] Dostupný zde: http://www.szpi.gov.cz/clanek/podminky-e-podani.aspx

S ohledem na kybernetickou bezpečnost je pak nutno zmínit i další aspekt důležitosti elektronické pošty, resp. její ochrany, a tím je fakt, že elektronická pošta je jedním z nejčastějších vektorů (tedy jakousi „bránou“) kybernetických útoků, a to bez ohledu na agendu či postavení správce konkrétního systému. Je pak nutné, aby každá organizační složka státu, kraj nebo hlavní město Praha měl zpracována opatření, která v konkrétních případech aplikuje. Rozsah a obsah těchto opatření závisí na specifikách jednotlivých případů.

Z pohledu zajišťování kybernetické bezpečnosti je nutno pamatovat na to, že se nejedná pouze o dostupnost systému, která může být ohrožena, u elektronické pošty je výrazně citelný i aspekt důvěrnosti a integrity. Právě v případě elektronické pošty tak může dojít jednak k úniku informací (osobní údaje, citlivé informace atp.), jednak k jejich modifikaci či podvrhu.

Jedná se o základní informační systém, který se bude u organizační složky státu, kraje nebo hlavního města Praha vyskytovat vždy.

5.3.4 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění kontrolní nebo inspekční činnosti anebo státního dozoru

Výkon státního dozoru a kontrolní a inspekční činnost jsou obvykle spojeny s výkonem spisové služby, v praxi však mohou existovat i samostatné systémy, prostřednictvím nichž k výkonu státního dozoru a kontrolní a inspekční činnosti, a tedy k výkonu veřejné moci, dochází. **Toto ustanovení se pak zaměřuje právě výhradně na tyto samostatné systémy, které jsou k této činnosti využívány.**

Znění tohoto ustanovení reaguje především na roztříštěnost označování kontrolních postupů v rámci českého právního řádu – lze se setkat s mnoha pojmy, jako např. státní dozor, kontrola, inspekce, ale také dohled, aj., přičemž většinou se jedná o instituty obdobné až totožné.

Jedná se o informační systém, který se u organizační složky státu, kraje nebo hlavního města Praha může samostatně vyskytovat, pokud nebude výkon této působnosti zajištěn výhradně spisovou službou.

5.3.5 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění výkonu veřejné moci při přípravě na krizové situace a jejich řešení

V případě přípravy na krizové situace a jejich řešení se jedná o krizovou situaci ve smyslu § 2 zákona č. 240/2000 Sb., krizový zákon (dále jen „krizový zákon“), tedy o mimořádnou událost podle zákona č. 239/2000 Sb., o integrovaném záchranném systému (mimořádnou událostí se rozumí škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací), o narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu.

V případě významného informačního systému k zajištění přípravy na krizové situace a jejich řešení se tedy jedná o informační systémy využívané při výkonu působnosti organizační

složky státu, kraje nebo hlavního města Praha k úkonům spojených se všemi aspekty přípravy na krizové situace, tedy především k úkonům zajišťujícím postupy podle krizového zákona, stejně jako k samotnému řešení a vyřešení těchto situací.

Jedná se o informační systém, který se u organizační složky státu, kraje nebo hlavního města Praha může samostatně vyskytovat, pokud nebude výkon této působnosti zajištěn výhradně spisovou službou.

5.3.6 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění výkonu spisové služby

Zájem na ochraně informačního systému, jehož prostřednictvím je vykonávána spisová služba, je dán především charakterem organizačních složek státu, krajů a hlavního města Prahy jakožto správních orgánů, jejichž zákonnou povinností je v každé věci zakládat spis[38] – **vedení spisu je esenciální a naprosto stěžejní složkou výkonu veřejné moci.**

Jedná se o základní informační systém, který se u organizační složky státu, kraje nebo hlavního města Praha bude vyskytovat vždy.

5.3.7 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění vedení úřední desky způsobem umožňujícím dálkový přístup

V souladu s § 26 odst. 1 správního řádu je každý správní orgán povinen zřídit úřední desku, která musí být nepřetržitě veřejně přístupná. Obsah úřední desky se zveřejňuje způsobem umožňujícím dálkový přístup. Na existenci a dostupnost úřední desky je navázán především výkon normotvorné činnosti správních orgánů (vydávání právních předpisů a dalších správních aktů), prostřednictvím úředních desek lze dále např. doručovat rozhodnutí, informovat veřejnost o záměru nakládat s veřejným majetkem nebo informovat o volbách a vyhlášení místního referenda.

Jedná se tak o základní informační systém, který se u organizační složky státu, kraje nebo hlavního města Praha bude vyskytovat vždy.

5.3.8 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění mezinárodní spolupráce

Mezinárodní spolupráce českých orgánů veřejné moci se zahraničními představiteli státní správy je zároveň reprezentací České republiky a funkčnosti veřejné správy v ní. Reputační riziko spojené s narušením bezpečnosti informací má tak dosah i za hranice České republiky.

Je ve veřejném zájmu, aby byla zachována důvěra našich zahraničních partnerů v to, že informace poskytované ze strany orgánů veřejné moci, potažmo tedy i Českou republikou jako

[38] srov. zejm. § 17 správního řádu nebo § 64 zákona č. 280/2009 Sb., daňový řád

státem, mají zachovánu integritu a důvěrnost a jsou dostupné, a nepřináší tak s sebou přes hranici zvýšená rizika pro kybernetickou bezpečnost těchto zahraničních partnerů.

Jedná se o informační systém, který se u organizační složky státu, kraje nebo hlavního města Praha může samostatně vyskytovat, pokud nebude výkon této působnosti zajištěn výhradně spisovou službou.

5.3.9 Informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění zadávání veřejných zakázek

Zadávání veřejných zakázek je vysoce formalizovaný postup, v jehož rámci jsou povinné osoby (zadavatelé ve smyslu § 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek) obecně povinny zadávat veřejné zakázky v zadávacím řízení. V rámci tohoto formalizovaného postupu je vyhotovována dokumentace o zadávacím řízení, kterou je zadavatel povinen uchovávat po dobu 10 let od ukončení zadávacího řízení nebo od změny závazku ze smlouvy.

Dokumentace o zadávacím řízení obsahuje osobní údaje, obchodní tajemství, někdy též utajované informace, informace o interních procesech, technickém řešení systémů, popis procesů, know-how, a to nejen zadavatelů, ale také dodavatelů ve formě nabídek, tzn. informace, které je nezbytné chránit před zneužitím. Vybrané dokumenty k zadávacímu řízení jsou povinně uveřejňovány na profilu zadavatele (elektronickém nástroji umožňujícím dálkový přístup).

Pro zadavatele dále platí povinnost zadávat veřejné zakázky elektronicky (srov. § 211 zákona č. 134/2016 Sb.), důraz je pak kladen na zajištění důvěrnosti nabídek a žádostí o účast a úplnosti údajů v nich obsažených. Pro některé subjekty platí povinné zadávání veřejných zakázek v Národním elektronickém nástroji, zbylé subjekty mohou využít jiné certifikované elektronické nástroje (jichž mohou a nemusí být sami správci nebo provozovateli).

Jedná se o informační systém, který se u organizační složky státu, kraje nebo hlavního města Praha může samostatně vyskytovat, pokud nebude výkon této působnosti zajištěn výhradně spisovou službou.

5.4 Určující kritéria pro významné informační systémy (§ 3 odst. 1 vyhlášky)

Pokud orgán veřejné moci identifikuje, že je správcem informačního systému, který není kritickou informační infrastrukturou ani informačním systémem základní služby a který využívá pro výkon své působnosti jako orgánu veřejné moci, bude v rámci hodnocení naplnění kritérií pro významný informační systém směřovat do vyhlášky o významných informačních systémech.[39]

[39] Organizační složky státu, kraje a hlavní město Praha pak nepostupují podle § 3 odst. 1 vyhlášky o významných informačních systémech v případě těch informačních systémů, které jsou uvedeny v § 2 odst. 1 této vyhlášky.

Orgány veřejné moci, které jsou organizačními složkami státu, kraji nebo hlavním městem Praha zhodnotí nejdříve naplnění § 2 odst. 1 vyhlášky (viz předchozí podkapitola 5.3). **Informační systémy neuvedené v § 2 odst. 1 vyhlášky organizační složky státu, kraje a hlavní město Praha posoudí podle § 3 odst. 1 této vyhlášky.**

Orgány veřejné moci, které nejsou organizačními složkami státu, kraji nebo hlavním městem Praha posoudí všechny své informační systémy podle § 3 odst. 1 vyhlášky.

Určující kritéria jsou stavěna jednoduchým způsobem – **§ 3 odst. 1 vyhlášky o významných informačních systémech stanovuje seznam dopadů, které by mohly nastat v případě, že by došlo v řešeném informačním systému k narušení bezpečnosti informací a zároveň by došlo k naplnění podmínky, že takový dopad nebude možné odvrátit bez vynaložení nepřiměřených nákladů.**

Je vhodné poznamenat, že všechna tato kritéria byla již obsahem § 4 původního znění vyhlášky o významných informačních systémech a v rámci novely vyhlášky došlo pouze k jejich jazykovému upřesnění.

5.4.1 Narušení bezpečnosti informací

Bezpečností informací se podle § 2 písm. c) zákona o kybernetické bezpečnosti rozumí *„zajištění důvěrnosti, integrity a dostupnosti informací a dat“.* Narušením bezpečnosti informací se tak rozumí narušení dostupnosti, důvěrnosti a integrity informací a dat v posuzovaném informačním systému a v rámci vyhlášky o významných informačních systémech se může projevit možnými dopady, které jsou uvedeny v § 3 odst. 1.

V rámci posuzování, zda některý z dopadů uvedených v seznamu může nastat, je potřeba mít na paměti několik zásad tohoto posuzování.

1. **Dopad stanovuje minimální hranici škod, které by mohly být narušením dostupnosti, důvěrnosti nebo integrity způsobeny.**
2. **Vůči dopadu je potřeba hodnotit každou z těchto domén bezpečnosti informací[40].**
3. **Každou z domén bezpečnosti informací je potřeba hodnotit samostatně, přičemž k naplnění dopadu stačí, když je narušena i jen jediná.**
4. **Dopady narušení jednotlivých domén bezpečnosti informací je potřeba hodnotit v souhrnu. K naplnění dopadových kritérií může dojít i tehdy, pokud dopady jednotlivých domén samy o sobě dopadová kritéria nenaplní, avšak součet dopadů všech tří domén požadovanou hranici překoná.**

[40] Dostupnost, jako vlastnost přístupnosti informací a dat, když jsou potřeba. Důvěrnost, jako vlastnost, že informace nebo data nejsou dostupná nebo nejsou odhalena neoprávněným jednotlivcům, entitám nebo procesům. Integrita, jako vlastnost, kdy informace nebo data nejsou změněna neautorizovaným subjektem nebo nechtěným způsobem.

5. **Při hodnocení je nutno hodnotit nejhorší možný scénář.**[41]
6. **Při hodnocení možného dopadu je nutno odhlédnout od zavedených bezpečnostních opatření.**[42]

Pouze za dodržení těchto zásad je možné hodnocení informačního systému provádět správně a dojít k objektivní identifikaci významného informačního systému nebo zjištění, že řešený informační systém žádné určující kritérium nenaplňuje.

5.4.2 Omezení či narušení – obecně

Před samotným rozborem jednotlivých dopadových scénářů je vhodné přiblížit pojem „omezení či narušení“, který se objevuje u prvních čtyř z nich.[43]

Obecně platí, že v případě omezení či narušení dochází k omezení či narušení rozsahu nebo kvality dané služby, informace, hospodaření nebo fungování.

Na omezení či narušení je tedy nutné pohlížet jak z kvantitativního, tak z kvalitativního pohledu.

Kvantitativní pohled omezení či narušení se projeví v různých podobách – výsledkem je, že nemusí být uspokojeni všichni potenciální odběratelé, může dojít k omezení dostupnosti, některé podpůrné nebo dílčí služby nejsou dostupné, může dojít k tomu, že nebude možné provádět potřebné úkony, některé podpůrné nebo dílčí služby bude nutno řídit náhradním způsobem apod.

Kvalitativní pohled omezení či narušení se projeví v jiných podobách – může docházet k výraznému nárůstu čekací doby pro potenciální odběratele, může dojít k úniku údajů obsažených v daném systému apod.

Všechny tyto aspekty je nutno při zhodnocení naplnění příslušného kritéria zvážit.

Pojem „omezení nebo narušení“ je také nutno vymezit proti pojmu „nedostupnost“, která znamená, že služba, informace, hospodaření nebo fungování není jen nějakým způsobem omezeno, ale je úplně nedostupné v plném rozsahu nebo kvalitě. Z toho důvodu je pro

---

[41] Zejm. je tedy potřeba zvažovat úplnou nedostupnost systému nebo dat v něm obsažených, únik nebo zveřejnění všech dat evidovaných v systému, změnu všech dat evidovaných v systému, úplné převzetí systému útočníkem a provádění neautorizovaných úkonů apod. Dopad je naplněn, i když je scénář k němu vedoucí málo pravděpodobný, pokud je objektivně realizovatelný.

[42] Všechna zavedená opatření mohou z různých důvodů selhat, stejně jako mohou být do budoucna z různých důvodů změněna či zrušena. Proto je potřeba hodnotit dopady narušení bezpečnosti informací a dat v informačním systému tak, jako by žádná bezpečnostní opatření nebyla zavedena. Navíc, pokud by bezpečnostní opatření byla součástí hodnocení, v případě zavedení dostatečných bezpečnostních opatření v důsledku plnění povinností ze zákona o kybernetické bezpečnosti by informační systém přestal splňovat tato kritéria a přestal by tak být významným informačním systémem. To by vedlo k neustálému cyklu spadání a vypadávání z regulace.

[43] Jednotným užitím pojmu „omezení nebo narušení“ dochází ke sjednocení terminologie s vyhláškou č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

naplnění dopadového scénáře, který spočívá v „*omezení nebo narušení*“, dostačující, aby služba, informace, hospodaření nebo fungování byly omezeny nebo narušeny, byť jen částečně.

5.4.3 Omezení či narušení poskytování služeb nebo informací orgánem veřejné moci veřejnosti [§ 3 odst. 1 písm. a)]

Prvním z dopadových scénářů je, že může v případě narušení bezpečnosti informací v řešeném informačním systému dojít k omezení či narušení poskytování služeb nebo informací orgánem veřejné moci veřejnosti, přičemž toto omezení nebo narušení služeb nebo informací nebude možné odvrátit bez vynaložení nepřiměřených nákladů.

Orgán veřejné moci může veřejnou moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Orgán veřejné moci tedy poskytuje služby a informace, avšak toto poskytování probíhá vždy pouze na základě konkrétního zákonného zmocnění. Zákonné zmocnění k poskytování určité služby (ať už jde pro službu určenou pro veřejnost, jiný orgán veřejné moci nebo pro interní potřebu), pak může být typicky dáno jak hromadně pro více orgánů veřejné moci zároveň[44], tak specificky pro konkrétní orgán veřejné moci[45].

Specifickou službou, která je však pro potřeby vyhlášky o významných informačních systémech zdůrazněna, je povinnost orgánu veřejné moci poskytovat informace.[46]

5.4.4 Omezení či narušení hospodaření orgánu veřejné moci [§ 3 odst. 1 písm. b)]

Druhým z dopadových scénářů je, že může v případě narušení bezpečnosti informací v řešeném informačním systému dojít k omezení či narušení hospodaření orgánu veřejné moci, přičemž toto omezení nebo narušení hospodaření nebude možné odvrátit bez vynaložení nepřiměřených nákladů.

Pojmem „hospodaření“ se obecně myslí správa hmotných prostředků orgánu veřejné moci. Obecně lze říci, že k naplnění tohoto kritéria dojde především, pokud by narušení bezpečnosti řešeného systému mělo negativní vliv na rozpočet daného orgánu veřejné moci, tedy došlo by k narušení stanoveného finančního modelu takového subjektu.

K takovým dopadům může dojít zejména ve dvou případech:

1. **Přímé omezení či narušení hospodaření orgánu veřejné moci**

   Určovaný systém je přímo spjat s hospodařením orgánu veřejné moci – prostřednictvím daného informačního systému orgán veřejné moci stanovuje rozpočet, stanovuje, kontroluje nebo jinými činnostmi zabezpečuje svůj finanční model apod. a z tohoto důvodu narušení dostupnosti, důvěrnosti nebo integrity takového

[44] např. srov. § 3 zákona č. 499/2004 Sb., o archivnictví a spisové službě
[45] např. srov. § 22 zákona o kybernetické bezpečnosti
[46] Především zákon č. 106/1999 Sb., o svobodném přístupu k informacím, a zákon č. 123/1998 Sb., o právu na informace o životním prostředí

systému může vést k změnám a škodám na činnostech spojených s hospodařením orgánu veřejné moci a vedoucích k jeho omezení nebo narušení.

2. **Nepřímé omezení či narušení hospodaření orgánu veřejné moci**

   Určovaný systém je nepřímo spjat s hospodařením orgánu veřejné moci – daný informační systém orgánu veřejné moci není určen k činnostem spojeným s hospodařením orgánu veřejné moci jako v předchozím případě, ale přesto narušení dostupnosti, důvěrnosti nebo integrity takového systému může vést ke změnám a škodám vedoucím k omezení nebo narušení hospodaření orgánu veřejné moci.

5.4.5 Jiné omezení či narušení fungování orgánu veřejné moci [§ 3 odst. 1 písm. c)]

Třetím z dopadových scénářů je, že může v případě narušení bezpečnosti informací v řešeném informačním systému dojít k jinému omezení či narušení fungování orgánu veřejné moci, než jakým je poskytování služeb nebo informací, anebo hospodaření orgánu veřejné moci, přičemž toto jiné omezení nebo narušení nebude možné odvrátit bez vynaložení nepřiměřených nákladů.

V případě třetího dopadového scénáře se jedná o pokrytí takových kategorií dopadů, které nejsou přiřaditelné ani k poskytování služeb, ani k hospodaření orgánu veřejné moci, a přesto se jedná o činnosti, které jsou potřeba, aby nebylo řádné fungování daného orgánu veřejné moci omezeno nebo narušeno. Cílem je zajistit, aby byla veřejná správa v České republice řádně vykonávána a účel, pro který byl orgán veřejné moci zřízen, nebyl prostřednictvím narušení dostupnosti, důvěrnosti nebo integrity řešeného systému, jakkoliv omezen nebo narušen. V tomto případě, více než kdekoliv jinde, budou tyto situace dány různě a vždy s ohledem na specifika každého individuálního orgánu veřejné moci.

5.4.6 Omezení či narušení fungování nebo hospodaření jiného orgánu nebo osoby podle § 3 zákona, popřípadě omezení či narušení poskytování služeb nebo informací veřejnosti tímto orgánem nebo osobou [§ 3 odst. 1 písm. d)]

Čtvrtým z dopadových scénářů je, že může v případě narušení bezpečnosti informací v řešeném informačním systému dojít k omezení či narušení fungování nebo hospodaření subjektu spadajícího pod zákon o kybernetické bezpečnosti, anebo že bude omezena či narušena schopnost subjektu spadajícího pod zákon o kybernetické bezpečnosti poskytovat služby nebo informace veřejnosti, přičemž toto omezení nebo narušení nebude možné odvrátit bez vynaložení nepřiměřených nákladů, ať už na straně orgánu veřejné moci nebo na straně dotčeného subjektu spadajícího pod zákon o kybernetické bezpečnosti.

Z důvodu možných propojení a vlivů určovaného systému i na jiné orgány veřejné moci než na orgán veřejné moci, který je jeho správcem, pamatuje vyhláška o významných informačních systémech i na situace, kdy k dopadům uvedeným ve všech třech výše uvedených případech dojde ne u správce řešeného systému, ale u jiného subjektu. Tento jiný subjekt je vymezen tak, že se musí jednat o subjekt spadající pod zákon o kybernetické bezpečnosti dle jeho § 3.

Přestože se může jednat o subjekty veřejného i soukromého práva, není zde tedy nutně dáno, že by se muselo jednat jen o jiné orgány veřejné moci, dá se předpokládat, že v případě tohoto kritéria bude možné omezení či narušení jiného významného informačního systému tou nejvíce relevantní situací. V případě, že tomu tak bude, bude nutné v zájmu dobré správy navázat vzájemnou spolupráci mezi orgány veřejné moci a na jejím základě dojít k potvrzení či vyvrácení naplnění tohoto kritéria.

5.4.7 Zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob [§ 3 odst. 1 písm. e)]

Pátým z dopadových scénářů je, že může v případě narušení bezpečnosti informací v řešeném informačním systému dojít k zásahu do osobního života nebo do práv fyzických nebo právnických osob postihujícího nejméně 50 000 osob, přičemž tento zásah nebude možné odvrátit bez vynaložení nepřiměřených nákladů.

Zásah do osobního života nebo do práv fyzických nebo právnických osob je kritériem zohledňujícím jednotlivce – adresáta veřejné moci (především občana).

Pojem osobní život byl použit, jelikož oproti jinému přípustnému pojmu „soukromí“ zahrnuje širší množinu případů, zejména zásah do sice osobního, ale nikoli soukromého života, např. osobní – profesní život. Na druhou stranu, právo na soukromí, resp. respekt k soukromému životu, který bude nejběžnější možnou ohroženou množinou, zahrnuje garanci sebeurčení ve smyslu zásadního rozhodování jedince o sobě samém, včetně rozhodování o uspořádání vlastního života. Oblastmi soukromého života je především lidská důstojnost, osobní čest, dobré jméno a také vnitřní potřeba sociálního kontaktu a sociálního začlenění daného jedince. K tomu navíc zásah do práv fyzických nebo právnických osob tuto množinu rozšiřuje o jakékoliv subjektivní právo, které by mohlo být negativně zasaženo v případě narušení bezpečnosti informací řešeného systému.

Zásahem je taková situace, která v návaznosti na narušení dostupnosti, důvěrnosti nebo integrity v řešeném systému může vést k tomu, že dojde k narušení osobního života (nebo některé jeho části, typicky soukromého života) nebo práv ve výše uvedeném smyslu.

Nejčastějším případem takového zásahu bude narušení důvěrnosti řešeného systému a veřejné vyzrazení obsažených informací, mimo jiné například osobních údajů, jejichž únik lze vnímat jako zásah do osobního života fyzických osob, o jejichž údaje jde (taková situace navíc již typicky nebude ani nijak odvratitelná).

Toto poměrně široce stanovené dopadové kritérium je omezeno na nutnost potenciálního zásahu více než 50 000 osob[47], přičemž při nutnosti hodnotit nejhorší možný scénář (viz výše)

[47] Tato hranice je stanovena v důsledku zaokrouhlení průměrné populace ve správním území obce s rozšířenou působností (členění České republiky dle § 66 zákona č. 128/2000 Sb., o obcích, a zákona č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností).

musí být jedním ze zvažovaných scénářů i vyzrazení všech údajů o všech osobách v rámci řešeného systému.

5.4.8 Ohrožení či narušení veřejného zájmu [§ 3 odst. 1 písm. f)]

Posledním z dopadových scénářů je, že může v případě narušení bezpečnosti informací v řešeném informačním systému dojít k ohrožení či narušení veřejného zájmu, přičemž toto omezení nebo narušení nebude možné odvrátit bez vynaložení nepřiměřených nákladů.

Tak, jako je výše uvedený zásah do osobního života nebo do práv fyzických nebo právnických osob kritériem zohledňujícím zájmy jednotlivce, zohledňuje ohrožení či narušení veřejného zájmu obecně chráněné zájmy. Cílem je tedy generálně pojmout možnost vlivu narušení bezpečnosti informací v řešeném systému na veřejnost a její zájmy jako celek. Veřejný zájem řadíme do kategorie neurčitých právních pojmů a jako takový vždy závisí na odborném posouzení orgánu veřejné moci v každém jednotlivém případě. Z tohoto důvodu je tedy nutné vždy v případě řešeného systému zvážit, zda narušení bezpečnosti informací v něm nemůže ohrozit nebo narušit veřejný zájem spjatý s výkonem té působnosti orgánu veřejné moci, pro kterou je využíván.

5.4.9 Možnost odvrátit omezení, narušení, zásah či ohrožení bez vynaložení nepřiměřených nákladů

S ohledem na poměrně široký rámec všech výše uvedených dopadových kritérií bude pro správnou identifikaci významného informačního systému stěžejní společná věta, která znění nového § 3 odst. 1 vyhlášky o významných informačních systémech uzavírá. Ta stanoví, že se o významný informační systém bude jednat pouze v případě, že uvedené situace, tedy kritéria uvedená v písm. a) až f), **nebude možné odvrátit bez vynaložení nepřiměřených nákladů.**

Je nutno zdůraznit, že nepříznivé dopady je nutno odvrátit vlastní činností organizace, a naopak není možné považovat za jejich odvrácení situaci, kdy činnost subjektu nahradí jiný orgán veřejné moci svou běžnou činností.

Vynaložení nepřiměřených nákladů jako neurčitý právní pojem musí být zkoumáno ve světle konkrétních okolností daného případu. Není možné ze strany Úřadu deklarovat přesnou výši, procento nebo jednoduchý vzorec, který by byl vždy za každé situace aplikovatelný u každého orgánu veřejné moci.

Lze však pro vyšší míru objasnění uvést následující příklad.

Orgán veřejné moci, který není organizační složkou státu, krajem ani hlavním městem Praha ročně vyřídí průměrně 20 žádostí o poskytnutí informací a 30 velmi stručných rozhodnutí ve správním řízení. Pro odpovědi na tyto žádosti a vydání těchto rozhodnutí používá informační systém – spisovou službu, avšak paralelně vede veškerou spisovou agendu i písemně.

Nejhorším možným scénářem z pohledu dostupnosti je úplná nedostupnost spisové služby v okamžiku, kdy by měl tento orgán vydat veškerá rozhodnutí a nemohl k jejich zpracování použít elektronickou spisovou službu. Pro tento případ má nastaven provizorní proces, který bude ve vztahu k jeho zaměstnancům znamenat 2 hodiny práce 2 osob navíc.

Nejhorším možným scénářem z pohledu integrity je úplné převzetí těchto systémů útočníkem a provedení neautorizovaných změn, z nichž nejvýznamnější by byla vydání rozhodnutí, která neměla být vydána. S ohledem na nápad práce orgánu se bude jednat o jednotky případů a formou postupů daných správním řádem[48] je za vynaložení práce 3 zaměstnanců po 2 dny orgán veřejné moci schopen případné nedostatky napravit.

Nejhorším možným scénářem z pohledu důvěrnosti je vyzrazení veškerých osobních údajů uchovávaných ve spisové službě, kterých však tento systém obsahuje velmi malé množství (nedosahuje ani na kritérium 50 000) a nejedná se ani o údaje povahy zvláště citlivé. V tomto případě není nutno vůbec posuzovat přiměřenost nákladů na zajištění náhradního opatření, protože k naplnění kritérií z povahy věci nemůže dojít.

Vzhledem k rozsahu systému tak náklady, které by bylo třeba vynaložit v případě jeho nefunkčnosti, nebudou nepřiměřené a daná spisová služba tak nenaplňuje kritéria podle § 3 odst. 1 vyhlášky o významných informačních systémech[49].

[48] Přezkum, obnova, oprava zřejmých nesprávností dle zákona č. 500/2004 Sb., správního řádu.

[49] Je potřeba upozornit, že toto neplatí pro posuzování podle § 2 odst. 1 vyhlášky, na tyto typové systémy spravované vyjmenovanými osobami (organizační složky státu a kraje a hlavní město Praha) se posouzení nepřiměřenosti nákladů nevztahuje.

ČÁST II
PO IDENTIFIKACI VÝZNAMNÉHO INFORMAČNÍHO SYSTÉMU

6 Základní povinnosti ze zákona o kybernetické bezpečnosti

Zatímco identifikace významného informačního systému je výhradní povinností správce, plnění zbylých zákonných povinností spojených se správou a provozem významného informačního systému je uloženo jak správci, tak provozovateli systému.

6.1 Implementace a provádění bezpečnostních opatření (§ 4 zákona o kybernetické bezpečnosti)

Správci a provozovatelé významných informačních systémů jsou povinni zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti jejich významného informačního systému a vést o nich bezpečnostní dokumentaci. Jedná se o hlavní povinnost obsaženou v zákoně o kybernetické bezpečnosti.

Bezpečnostní opatření jsou specifikována v § 5 zákona o kybernetické bezpečnosti a dělí se na organizační a technická. Jednotlivá opatření blíže specifikuje vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „vyhláška o kybernetické bezpečnosti“).

6.2 Hlášení kontaktních údajů (§ 16 zákona o kybernetické bezpečnosti)

Správci a provozovatelé významných informačních systémů mají podle § 16 odst. 2 písm. b) zákona o kybernetické bezpečnosti nahlásit Úřadu své kontaktní údaje.

Formulář pro hlášení kontaktních údajů a další informace naleznete na této adrese:

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

Kontaktní údaje pak obsahují především údaje o fyzické osobě, která je za orgán oprávněna jednat ve věcech upravených zákonem o kybernetické bezpečnosti. Jako tato osoba by ve formuláři měla být uvedena osoba odpovědná za tento systém, nejlépe garant, který má rozhodovací pravomoc v souvislosti se systémem. Samozřejmě je možné uvést osob více (např. administrátory, manažera kybernetické bezpečnosti apod.). Součástí formuláře jsou nejen kontaktní údaje k systému, ale jsou vyžadovány také základní informace o systému, rozsazích IP adres, které používá, a další informace uvedené ve formuláři hlášení kontaktních údajů.

V případě potřeby je možné využít také návod pro vyplnění formuláře hlášení kontaktních údajů, který naleznete na stejné adrese.

Vyplněný formulář s hlášením kontaktních údajů zašlete do datové schránky Úřadu, ISDS: zzfnkp3 nebo elektronicky podepsané na e-mail regulace@nukib.cz.

V případě, že informační systém, který byl identifikovaný jako významný informační systém již za původního znění vyhlášky o významných informačních systémech, naplní kritéria pro významný informační systém i podle nového znění této vyhlášky, a Úřadu byly k tomuto významnému informačnímu sytému hlášeny kontaktní údaje, **nemusí orgán veřejné moci hlásit z důvodu nabytí účinnosti nového znění vyhlášky kontaktní údaje znovu.** Je však možné se na Úřad z tohoto důvodu obrátit a upřesnit obsah hlášení tak, aby lépe vyhovoval a byl pro praktické použití lépe použitelný.

V případě, že informační systém identifikovaný jako významný informační systém (ať už za původního, nebo i nového znění vyhlášky), ke kterému byly kontaktní údaje hlášeny Úřadu, **ve výjimečných případech přestane naplňovat daná kritéria, je nutno tuto informaci Úřadu sdělit a odůvodnit.** Teprve poté dojde k odstranění údajů z evidence kontaktních údajů. Tento postup je potřeba použít také v případě, že je významný informační systém uveden v příloze č. 1 původního znění vyhlášky o kybernetické bezpečnosti. Přestože dnem nabytí účinnosti nového znění vyhlášky dne 1. ledna 2021 dojde k odstranění přílohy č. 1, nemá toto odstranění přílohy vliv na vedení v ní uvedených systémů jako významných informačních systémů.

6.3 Hlášení kybernetických bezpečnostních incidentů (§ 8 zákona o kybernetické bezpečnosti)

Správci a provozovatelé významných informačních systémů mají podle § 8 odst. 1 a odst. 4 zákona o kybernetické bezpečnosti povinnost hlásit kybernetické bezpečnostní incidenty, a to Vládnímu CERT (který je součástí Úřadu). K provedení hlášení slouží elektronický formulář, který je k dispozici ke stažení na internetových stránkách Úřadu.

Formulář pro hlášení kybernetických bezpečnostních incidentů, postup hlášení a další informace naleznete na této adrese:

https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/

Správcova povinnost nahlásit kybernetický bezpečnostní incident bez zbytečného odkladu je splněna i tehdy, pokud byl kybernetický bezpečnostní incident hlášen provozovatelem systému.

6.4 Provádění opatření (§ 11 až § 14 zákona o kybernetické bezpečnosti)

Opatřeními se rozumí úkony, jichž je třeba k ochraně systémů před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

Opatřeními jsou varování (§ 12), reaktivní opatření (§ 13) a ochranné opatření (§ 14).

Správci a provozovatelé významných informačních systémů jsou povinni, ať už v případě reaktivních nebo ochranných opatření přímo, tak v případě varování nepřímo, provádět opatření vydaná Úřadem.

V případě uloženého reaktivního opatření jsou správci a provozovatelé významných informačních systémů povinni bez zbytečného odkladu oznámit Úřadu jeho provedení a výsledek.

Formulář pro oznámení způsobu provedení reaktivního opatření a další informace naleznete na této adrese:

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

7 Lhůty pro plnění povinností

Pro plnění jednotlivých zákonných povinností (uvedených výše) jsou zákonem o kybernetické bezpečnosti stanoveny lhůty. Při počítání lhůt podle § 31 zákona o kybernetické bezpečnosti je především třeba brát v potaz, že významným informačním systémem se daný informační systém stává okamžikem objektivního naplnění definice a neprobíhá zde žádný proces určování, ať už ze strany Úřadu, nebo ze strany daného orgánu veřejné moci.

Ustanovení § 31 zákona o kybernetické bezpečnosti uvádí:

Správci a provozovatelé významných informačních systémů

a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů,

b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 4 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a

c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému.

Jak vidno, zákon o kybernetické bezpečnosti spojuje počátek běhu lhůt pro plnění povinností s okamžikem objektivního naplnění určujících kritérií. Je přitom lhostejno, zda se bavíme o nově vznikajícím nebo upravovaném systému (který svým vznikem nebo úpravou naplní již účinná určující kritéria), nebo o systému existujícím již před přijetím nové právní úpravy, u něhož k naplnění určujících kritérií dojde vstupem nové právní úpravy (tj. nových určujících kritérií) v účinnost. Z tohoto důvodu platí, že pokud daný informační systém existuje v době, kdy vstupují v účinnost určující kritéria definující významný informační systém, začínají tímto okamžikem plynout lhůty dané ustanovením § 31 zákona o kybernetické bezpečnosti. Kdy bude proveden proces identifikace významného informačního systému z pohledu orgánu veřejné moci v pozici správce významného informačního systému, nemá na plynutí lhůt žádný vliv. Pokud tedy správce významného informačního systému povinnost identifikovat významné informační systémy podcení, může dojít do situace, kdy v momentě provedení identifikace významného informačního systému již lhůty dané § 31 zákona o kybernetické bezpečnosti uplynuly.

Je také potřeba si uvědomit, že § 31 zákona o kybernetické bezpečnosti stanoví lhůty pouze pro plnění některých povinností, ostatní povinnosti ze zákona o kybernetické bezpečnosti, pro které lhůta stanovena není, je potřeba plnit okamžitě. To se týká zejména provádění reaktivního a ochranného opatření.

Stejně tak je potřeba akcentovat, že pokud byl určitý informační systém identifikován jako významný informační systém již před novelou vyhlášky o významných informačních systémech a tento systém naplňuje i nová určující kritéria, nedochází k žádnému novému přeurčení či k novému naplnění určujících kritérií. Tento systém je významným informačním

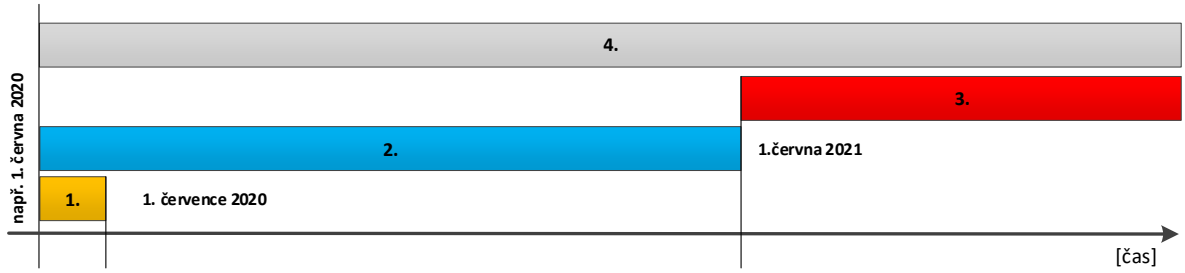
systémem od okamžiku původní identifikace a od tohoto okamžiku se také počítají lhůty pro plnění zákonných povinností.

V praxi tedy může nastat několik situací, při nichž je potřeba sledovat stav informačního systému s ohledem na původní znění vyhlášky o významných informačních systémech[50]:

1. **Informační systém je významným informačním systémem již za původního znění, a je jím rovněž podle nového znění.**

V tomto případě dochází pouze k formálním úpravám (např. zformalizování posouzení daného systému a zavedení záznamu takového posouzení do seznamu apod.), nicméně k žádným změnám statusu daného významného informačního systému nedochází – z tohoto důvodu nevzniká žádný důvod k novému počítání lhůty, lhůta plynula již podle původního znění.

Situaci č. 1 znázorňuje toto schéma (data jsou pouze ilustrační):



Orgán veřejné moci spustil v pozici správce dne 1. června 2020 informační systém. Tento informační systém objektivně naplnil k tomuto dni určující kritéria daná původním zněním vyhlášky. Lhůta pro hlášení kontaktních údajů uplynula po 30 dnech, tedy 1. července 2020 (označeno „1." a znázorněno žlutě). Lhůta 1 roku pro implementaci vybraných povinností (hlášení kybernetických bezpečnostních incidentů NÚKIB podle § 8 odst. 1 zákona o kybernetické bezpečnosti a zavedení bezpečnostních opatření podle § 4 odst. 2 téhož zákona) uplyne 1. června 2021 (označeno „2." a znázorněno modře). Jakmile tato lhůta uplyne, musí orgán veřejné povinnosti plnit zmíněné povinnosti a Úřad má možnost jejich plnění kontrolovat (označeno „3." a znázorněno červeně). Ostatní povinnosti dané zákonem o kybernetické bezpečnosti, především provádění reaktivních a ochranných opatření a možnost jejich kontroly, pro které není § 31 zákona o kybernetické bezpečnosti stanovena lhůta, je nutné plnit okamžitě (označeno „4." a znázorněno šedě).

Přijetí nového znění vyhlášky nemá na tuto situaci žádný vliv – lhůty pro plnění povinností nepočínají běžet znovu.

[50] *„Původním zněním"* se v tomto případě myslí znění vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, mezi 19. prosincem 2014 a 31. prosincem 2020. *„Novým zněním"* se myslí Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ze znění novely č. 360/2020 Sb., tedy od 1. ledna 2021 dále.

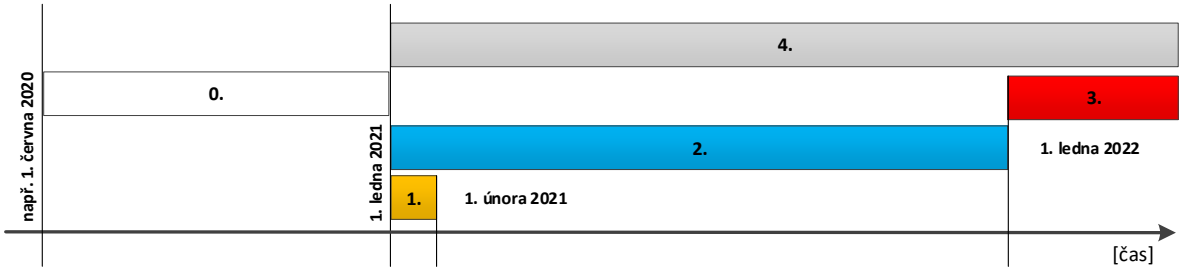
2. Informační systém není významným informačním systémem za původního znění, ale bude jím podle nového znění.

V případě, že informační systém doposud nenaplňoval určující kritéria, ale s novou právní úpravou je naplní, bude se daná lhůta počítat podle data vstupu takové právní úpravy v účinnost (v případě § 3 odst. 1 vyhlášky o významných informačních systémech tomu tedy bude od 1. ledna 2020, v případě § 2 odst. 1 bude účinnost nabíhat postupně v následujících třech letech).

Tato situace nastane zejména v případě pořizování zcela nových informačních systémů.

Naopak pokud orgán veřejné moci v pozici správce informačního systému u řešeného systému neprovedl podle původního znění identifikaci správně a tento řešený systém měl naplňovat kritéria daná již původním zněním, počítá se lhůta od doby objektivního naplnění kritérií podle původního znění (jako by tomu bylo podle výše uvedené 1. situace).

Situaci č. 2, v případě, kdy orgán veřejné moci v pozici správce spustil informační systém za doby účinnosti původního znění, ten však podle původního znění nenaplnil kritéria a naplní je až za nového znění, znázorňuje toto schéma (data jsou pouze ilustrační):

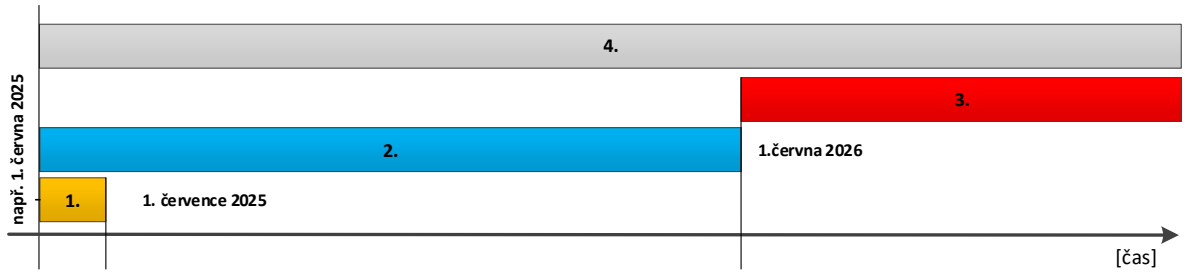


Orgán veřejné moci spustil v pozici správce dne 1. června 2020 informační systém. Tento informační systém objektivně nenaplnil k tomuto dni určující kritéria daná původním zněním vyhlášky. S účinností nového znění však tento informační systém objektivně naplnil kritéria a stal se významným informačním systémem (označeno „0.“ a znázorněno bíle). Lhůta pro hlášení kontaktních údajů uplyne po 30 dnech, tedy 1. února 2021 (označeno „1.“ a znázorněno žlutě). Lhůta 1 roku pro implementaci vybraných povinností (hlášení kybernetických bezpečnostních incidentů NÚKIB podle § 8 odst. 1 zákona o kybernetické bezpečnosti a zavedení bezpečnostních opatření podle § 4 odst. 2 téhož zákona) uplyne 1. ledna 2022 (označeno „2.“ a znázorněno modře). Jakmile tato lhůta uplyne, musí orgán veřejné moci plnit zmíněné povinnosti a Úřad má možnost jejich plnění kontrolovat (označeno „3.“ a znázorněno červeně). Ostatní povinnosti dané zákonem o kybernetické bezpečnosti, především provádění reaktivních a ochranných opatření a možnost jejich kontroly, pro které není § 31 zákona o kybernetické bezpečnosti stanovena žádná lhůta, je nutné plnit okamžitě (označeno „4.“ a znázorněno šedě).

Přijetí nového znění vyhlášky má na tuto situaci ten vliv, že od 1. ledna 2020 se systém stává významným informačním systémem a počínají tím běžet lhůty pro plnění povinností. Datum,

kdy orgán veřejné moci v pozici správce systému provede jeho identifikaci, na tuto situaci nemá žádný vliv.

Situaci č. 2, v případě, kdy orgán veřejné moci v pozici správce spustí informační systém až za nového znění, znázorňuje toto schéma (data jsou pouze ilustrační):



Orgán veřejné moci spustil v pozici správce dne 1. června 2025 informační systém. Tento informační systém objektivně naplnil k tomuto dni určující kritéria daná novým zněním vyhlášky. Lhůta pro hlášení kontaktních údajů uplyne po 30 dnech, tedy 1. července 2025 (označeno „1.“ a znázorněno žlutě). Lhůta 1 roku pro implementaci vybraných povinností (hlášení kybernetických bezpečnostních incidentů NÚKIB podle § 8 odst. 1 zákona o kybernetické bezpečnosti a zavedení bezpečnostních opatření podle § 4 odst. 2 téhož zákona) uplyne 1. června 2026 (označeno „2.“ a znázorněno modře). Jakmile tato lhůta uplyne, musí orgán veřejné povinnosti plnit zmíněné povinnosti a Úřad má možnost jejich plnění kontrolovat (označeno „3.“ a znázorněno červeně). Ostatní povinnosti dané zákonem o kybernetické bezpečnosti, především provádění reaktivních a ochranných opatření a možnost jejich kontroly, pro které není § 31 zákona o kybernetické bezpečnosti stanovena žádná lhůta, je nutné plnit okamžitě (označeno „4.“ a znázorněno šedě).

3. **V případě, že informační systém doposud naplňoval určující kritéria, ale s novou právní úpravou je již nenaplní, přestane být významným informačním systémem.**

Tato situace je s ohledem na důvody a provedení nového znění, jehož cílem bylo zpřesnit původní znění, avšak neměnit jeho rozsah, velmi nepravděpodobná.

4. **Informační systém není významným informačním systémem za původního znění a nebude jím ani podle nového znění.**

V tomto případě daný informační systém nebyl a nadále nebude významným informačním systémem a lhůty pro plnění povinností není nutné řešit.

Další informace

Internetové stránky Úřadu

https://www.nukib.cz

Podpůrné materiály k celé problematice zákona o kybernetické bezpečnosti naleznete v aktuální podobě na internetových stránkách Úřadu v sekci

KYBERNETICKÁ BEZPEČNOST – REGULACE A KONTROLA – PODPŮRNÉ MATERIÁLY

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Formuláře

Elektronické formuláře ke stažení

Formulář pro hlášení kontaktních údajů

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

Formulář pro hlášení kybernetického bezpečnostního incidentu

https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/

Formulář pro oznámení způsobu provedení reaktivního opatření

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

Zákony a jiné relevantní právní předpisy

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, v aktuálním znění

Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, v aktuálním znění

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), v aktuálním znění

Přílohy

Příloha č. 1: Judikatura týkající se definice orgánu veřejné moci

Ústavní soud formuluje obsah tohoto pojmu již od roku 1993, přičemž navazuje na judikaturu Ústavního soudu České a Slovenské Federativní Republiky. Ten v rámci svého usnesení ze dne 19. března 1992, sp. zn. II. ÚS 18/92, stanovil, že *„Východiskem pro vymezení pojmu „orgán veřejné moci“ je vztah veřejného a soukromého práva. Za právo veřejné soud považuje tu oblast práva, v níž jsou vztahy založeny na nerovnosti zúčastněných subjektů, k soukromému právu patří vztahy založené na jejich rovnosti. Veřejná moc je taková, která autoritativně rozhoduje o právech a povinnostech subjektů, ať přímo nebo zprostředkovaně. Subjekt, o jehož právech nebo povinnostech rozhoduje orgán veřejné moci, není v rovnoprávném postavení s tímto orgánem a obsah rozhodnutí tohoto orgánu není dán na jeho vůli. Veřejnou moc vykonává stát především prostřednictvím orgánů moci zákonodárné, výkonné, soudní a dále ji mohou vykonávat další subjekty (např. korporace). Jiný subjekt než stát jedná jako orgán veřejné moci, jestliže rozhoduje v oblastech, ve kterých mu stát zákonem svěřil působnost rozhodovat o právech a povinnostech jiných osob a tato rozhodnutí jsou státní mocí vynutitelná, či do těchto práv a povinností zasahovat. Jiný orgán jedná jako orgán veřejné moci ve smyslu čl. 6 úst. zák.* [čl. 6 ústavního zákona č. 91/1991 Sb., o Ústavním soudu České a Slovenské Federativní Republiky: „Ústavní soud rozhoduje o ústavních stížnostech proti opatřením, pravomocným rozhodnutím nebo jiným zásahům orgánů veřejné moci, jestliže stěžovatel tvrdí, že jimi byly porušeny jeho základní práva a svobody, zaručené ústavním zákonem Federálního shromáždění nebo mezinárodními smlouvami uvedenými v čl. 2 písm. b). Podmínky stanoví zákon Federálního shromáždění.“] *při rozhodování o základních právech nebo svobodách tehdy, je-li účastenství v něm nutnou podmínkou pro realizaci takového práva nebo svobody a nelze-li právo nebo svobodu uplatnit jinak. Jednání orgánu, který může vystupovat jako nositel veřejné moci, nejsou projevem této moci, vystupuje-li jako osoba soukromého práva. Hranice veřejné moci končí tam, kde začíná moc soukromá.“*

Na toto usnesení navázal ještě v témže roce usnesením ze dne 9. června 1992, sp. zn. 191/92, kde potvrdil výše uvedené závěry. Na výše uvedené závěry navázal po rozdělení Československa a zániku Ústavního soudu České a Slovenské Federativní Republiky také nově zřízený Ústavní soud České republiky, a to hned v listopadu 1993, kdy výše uvedené shrnul v rámci usnesení ze dne 25. listopadu 1993, sp. zn. II. ÚS 75/93, přičemž v rámci řešeného případu se jednalo o to, zda je soudní znalec v postavení orgánu veřejné moci. Ústavní soud došel k následujícímu: *„Veřejnou mocí se rozumí taková moc, která autoritativně rozhoduje o právech a povinnostech subjektů, ať již přímo, nebo zprostředkovaně. Subjekt, o jehož právech nebo povinnostech rozhoduje orgán veřejné moci, není v rovnoprávném postavení s tímto orgánem a obsah rozhodnutí tohoto orgánu nezávisí od vůle subjektu. Za orgán veřejné moci nelze proto z tohoto pohledu považovat soudního znalce, jehož posudek může sloužit*

nejvýše jako podklad pro určité rozhodnutí nebo opatření, a to v projednávané věci právnické osoby.“

O dva roky později se Ústavní soud v rámci usnesení ze dne 23. června 1995, sp. zn. II. ÚS 86/95, při definici orgánu veřejné moci výslovně odvolal na výše uvedená usnesení Ústavního soudu České a Slovenské Federativní Republiky. Tímto usnesením se Ústavní soud také vyjádřil ke konkrétní situaci, zda v případě habilitačního řízení vystupuje vědecká rada jako orgán veřejné moci. K tomu Ústavní soud uvedl: „*Vzhledem k tomu, že v dané věci jde o výsledek habilitačního řízení, v němž navrhovatel vystupoval jako uchazeč, resp. kterého se zúčastnil na základě svobodného rozhodnutí, tedy na základě vlastního přivolení (§ 1 vyhl. č. 447/1990 Sb.), a vzhledem k tomu, že završující akt v kladném případě, tj. jmenování, nemá zcela zjevně povahu autoritativního rozhodnutí, čímž ji nemůže mít ani jeho negativní podoba, má Ústavní soud za to, že nejde v případě rozhodnutí vědecké rady o zásah orgánu veřejné moci. Ostatně, že se o zásah orgánu veřejné moci nejedná, plyne i ze skutečnosti, že navrhovateli nic nebrání, aby i nadále setrvával jak na svých metodách bádání, tak i učiněných závěrech. Ne v neposlední řadě dlužno dodat, že ze samého smyslu zákonů (zák. č. 172/1990 Sb. a vyhl. č. 447/1990 Sb.), podle kterých řízení proběhlo a které stanoví, že posláním vysokých škol je chránit a rozvíjet vzdělání, přispívat ke zvyšování vědecké, technické a hospodářské úrovně v podmínkách, zaručujících svobodu vědeckého bádání s tím, že vysokým školám přísluší výhradní právo na udělování akademických titulů, taktéž plyne, že výsledek habilitačního řízení není autoritativním výrokem, nýbrž výkonem práva dle čl. 15 Listiny. Za této situace má Ústavní soud za to, že nejde o rozhodnutí orgánu veřejné moci (…).*

V řadě usnesení Ústavního soudu došlo v prosinci roku 1998 také na vydání nálezu Ústavního soudu. Nález Ústavního soudu ze dne 1. prosince 1998, sp. zn. I. ÚS 41/98, akcentoval skutečnost, že prvky veřejného a soukromého práva nelze vždy jednoznačně oddělovat. K této problematice uvádí následující: „*V moderní společnosti se nezřídka prolínají prvky veřejného a soukromého práva tak, že nelze zcela jednoznačně veškerou činnost té či oné instituce označit pouze za veřejnoprávní nebo pouze za soukromoprávní. Lze si představit, že určitá instituce podle povahy konkrétní činnosti může v určitých vztazích vystupovat jako soukromoprávní, v jiných jako veřejnoprávní subjekt. Je proto třeba vážit, o jaký konkrétní druh té které činnosti se jedná (…). Nesplnění oznamovací povinnosti vůči Ministerstvu financí a v důsledku toho uložení sankce ze strany burzovní komory obsahuje nepochybně prvek rozhodování o právech a povinnostech právnické osoby v oblasti veřejné správy. Jedná se přinejmenším o nepřímý výkon státní správy (…). Institut „veřejné moci“ je vnímán jako institut, zahrnující přímou „moc státní“ a dále „zbývající veřejnou moc“. Státní mocí disponuje sám stát a zabezpečuje ji prostřednictvím svého zvláštního aparátu. Tzv. zbývající veřejná moc je v příslušném rozsahu svěřena subjektům nestátního charakteru ke správě veřejných záležitostí, je od státní moci v jistém smyslu odvozena a nemůže s ní být v rozporu. S veřejnou mocí přitom souvisí neoddělitelně nerovnost v postavení subjektů ve vztazích touto mocí ovládaných.“*

Dalším konkrétním případem, kdy Ústavní soud rozhodoval o tom, zda se jedná o orgán veřejné moci či nikoliv, je závěr usnesení Ústavního soudu ze dne 24. února 1999, sp. zn. I. ÚS 505/98, a případ funkcionáře orgánu veřejné moci v rámci služebního poměru. V tomto případě Ústavní soud uvádí: „*Za akt orgánu veřejné moci se považuje také jednání konkrétního funkcionáře orgánu veřejné moci, pokud rozhoduje o subjektivních právech a povinnostech subjektů. Pokud však funkcionář orgánu veřejné moci vykonává zákonem založené právo a povinnost "řídit" podřízené [§ 50 písm. a) zákona č. 154/ 1994 Sb., o Bezpečnostní informační službě (dále jen "zákon")], nejedná jako orgán veřejné moci, resp. nejde o rozhodování orgánu veřejné moci v uvedeném smyslu. Nerozhoduje se o subjektivních právech a povinnostech nepodřízených subjektů, ale jde o "řízení" podřízených individuálními pokyny a rozkazy nadřízeného v rámci právního vztahu dobrovolně založeného na základě žádosti o přijetí do služebního poměru (§ 23 zákona); jde tedy o interní služební vztah nadřízenosti a podřízenosti dobrovolně přijatý.*“

Vedle Ústavního soudu se touto otázkou zabýval také Nejvyšší soud, který v rámci svého rozsudku ze dne 31. ledna 2007, sp. zn. 25 Cdo 312/2005, řešil otázku odpovědnosti státu za škodu způsobenou nezákonným rozhodnutím či nesprávným úředním postupem. V rozsudku uvádí: „*Tento pojem* (výkon veřejné moci) *není v zákoně blíže vymezen, nicméně obvykle je za její výkon považováno vynucování vůle vyjadřující veřejný (státní či obecní) zájem vůči jednotlivcům, sociálním skupinám i celé společnosti. Dochází přitom zpravidla k rozhodování o právech, právem chráněných zájmech či povinnostech těchto subjektů, přičemž stát není s nimi v rovném postavení, nýbrž jedná z tzv. vrchnostenské pozice, kdy disponuje mocenskými prostředky, aby si vytvořil podmínky pro rozhodnutí a aby plnění jím uložených povinností vymohl.* (…) *Z tohoto pojetí výkonu veřejné moci, s nímž se jedině spojuje objektivní odpovědnost státu za škodu podle zákona č. 82/1998 Sb., vychází též ustálenou soudní judikaturou respektovaná zásada, že při nakládání se státním majetkem stát ve vrchnostenské pozici vůči nabyvateli nevystupuje* (…) *Postup příslušných orgánů státu při prodeji státního majetku je sice postupem státu, nicméně nikoliv státu jako nositele veřejné moci, ale státu jako dosavadního vlastníka nabízeného majetku, jehož dispozice je výrazem a důsledkem vlastníkovy vůle (srov. obdobně např. usnesení Ústavního soudu ze dne 9. 4. 1998, sp. zn. III. ÚS 380/97, publikované ve Sbírce nálezů a usnesení Ústavního soudu, sv. 10, pod č. 27). Výkonem veřejné moci (státní moci) není nakládání státu státním majetkem, a to ani v případě, že při něm dojde k porušení stanovených pravidel (srov. již citovaný nález Ústavního soudu sp. zn. II. ÚS 93/99), tedy např. i při uzavírání kupní smlouvy o prodeji věci ve vlastnictví státu. Tyto principy lze obdobně promítnout i do případu nakládání s majetkem státu podle zákona č. 219/2000 Sb., jak tomu bylo i v daném případě, ostatně samo znění tohoto zákona tomu nasvědčuje.*“ Postavením orgánu veřejné moci v majetkových případech a ve vztahu k odpovědnosti za škodu se zabýval i Ústavní soud v rámci svého usnesení ze dne 27. října 2015, sp. zn. I. ÚS 299/15, kde potvrdil výše uvedené závěry.

Příloha č. 2: Vzorový seznam informačních systémů podle § 3 odst. 2 vyhlášky o významných informačních systémech

Seznam informačních systémů orgánu veřejné moci podle § 3 odst. 2 vyhlášky č. 317/2014 Sb. (*Ministerstvo*)				**Verze**	*1.0*	**Vyplnil/a**	*Anna Nováková* *manažer kybernetické bezpečnosti*
				Poslední změna	*1. ledna 2021*		
Pořadové číslo	**Označení informačního systému**	**Výkon působnosti podporovaný systémem**	**Významný informační systém**	**Naplněné kritérium**	**Důvod (ne)naplnění definice významného informačního systému**		**Komentář**
Vzor 1	*Spisová služba*	*Vedení správních řízení, spisová služba*	*ANO*	*§ 2 odst. 1 písm. a)* *§ 3 odst. 1 písm. c)*	*Bez systému nelze vykonávat základní činnosti. Nahrazení není možné bez vynaložení nepřiměřených nákladů (…)*		
Vzor 2	*Rejstřík X*	*Zákonná povinnost vedení rejstříku podle zákona č. X*	*NE*	---	*Rejstřík X je součástí určené kritické informační infrastruktury XY. (…)*		
Vzor 3	*Docházkový systém*	*Vedení docházky v rámci Ministerstva*	*NE*	---	*Neslouží k výkonu působnosti orgánu veřejné moci.*		
1.							
(…)	(…)	(…)	(…)	(…)	(…)		(…)
Datum	*5. ledna 2021*	**Schválil/a a podepsal/a**		*Jan Novák, ministr*	*Jan Novák, v. r.*		**Interní**

Pozn.: Příklady možného vyplnění jsou psány *kurzívou*.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
1. 12. 2020	1.0	Odb. regulace	Vytvoření dokumentu