NÚKIB

PROVOZOVATEL INFORMAČNÍHO NEBO KOMUNIKAČNÍHO SYSTÉMU

podle § 2 písm. g) zákona o kybernetické bezpečnosti

Verze 3.2, platná ke dni 22. 12. 2022

Obsah

Úvod

Dokument obsahuje informace o institutu provozovatele informačního nebo komunikačního systému kritické informační infrastruktury, významného informačního systému nebo informačního systému základní služby (dále také jen „systém“) podle § 2 písm. g) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon“ nebo „zákon o kybernetické bezpečnosti“) zavedeného do tohoto zákona zákonem č. 104/2017 Sb., kterým se mění zákon o informačních systémech veřejné správy, zákon o kybernetické bezpečnosti, a některé další zákony.

Verze 3.0 tohoto dokumentu vznikla za účelem reflektovat a zpřesnit výklad pojmu „provozovatel informačního nebo komunikačního systému“ podle § 2 písm. g) zákona, a to na základě zkušeností s praktickými problémy aplikace tohoto zákonného institutu. Institut byl od své účinnosti (1. července 2017) doplněn nejen novelou zákona o kybernetické bezpečnosti účinnou k 1. srpnu 2017, ale jeho praktickou aplikaci ovlivnil také obsah vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat o kybernetické bezpečnosti (dále jen „vyhláška o kybernetické bezpečnosti), přičemž právě ustanovení § 8 této vyhlášky má velký vliv na informace obsažené v tomto dokumentu.

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

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.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze.

1 Definice provozovatele systému podle § 2 písm. g) zákona

1.1 Podstatné náležitosti definice provozovatele systému

Provozovatelem systému se podle § 2 písm. g) zákona o kybernetické bezpečnosti rozumí **„orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“.**

První podstatnou náležitostí je, že se jedná o orgán nebo osobu **„zajišťující“** určitou činnost. S ohledem na nutnost průběhu této činnosti **nelze za zajišťování ve výše uvedeném smyslu považovat jednotlivé a jednorázové dodávky technických a programových prostředků, bez dalších navazujících** (typicky servisních nebo provozních) **činností. Stejně tak se nebude jednat o dodávky nebo služby, které jsou sice poskytovány opakovaně stejným dodavatelem, ale jsou svou povahou jednorázové, nejedná se o konstantní zajišťování určité činnosti a poskytování těchto dodávek nebo služeb není z povahy věci** (zejm. s ohledem na předmět plnění) **vázáno na jednoho konkrétního dodavatele.**[1]

Cílem zajišťované činnosti je **„funkčnost“** technických a programových prostředků. **Bude se tedy jednat o činnosti spočívající např. v zajištění oprav, aktualizace softwaru, ale také např. zajištění služeb pro zachování minimální úrovně poskytovaných služeb,** která je přijatelná pro užívání, provoz a správu systému po kybernetickém bezpečnostním incidentu nebo po selhání tohoto systému, a další činnosti, jejichž cílem je zachování technických a programových prostředků v požadované kvalitě. **Pod tento pojem spadá také implementace technických nebo programových prostředků**, obvykle spojená s dodávkami hardwaru nebo softwaru. Naopak pouze tyto dodávky bez implementace zajišťováním funkčnosti nebudou, a navíc budou typicky jednorázové (viz výše). Zajišťování funkčnosti technických a programových prostředků tvořících systém je třeba chápat jako **aktivní činnost** směřující k zabezpečení řádného fungování technických a programových prostředků tvořících systém tak, aby systém mohl poskytovat služby, pro které byl pořízen. Pokud jde tedy např. o aktualizace programových prostředků, jež jsou součástí systému, vydavatel aktualizace bude provozovatelem pouze v případě, že se současně aktivně podílí na implementaci aktualizace do produkčního prostředí. Naopak pokud vydavatel aktualizaci pouze zpřístupní a pro její samotnou implementaci do systému je třeba provést další úkony (stáhnout, otestovat a následně nainstalovat, nebo aktivně povolit automatickou aktualizaci), **které však**

[1] Příkladem může být situace, kdy existuje praxe, že opravy (formou opakujících se jednorázových dodávek) zajišťuje stále stejný dodavatel, avšak neexistuje např. rámcová smlouva, která by stanovovala jednotnou úroveň poskytovaných služeb nebo zajišťovala, že opravy bude i v budoucnu provádět stále tento stejný dodavatel. Naopak za jednorázovou dodávku nebo službu, a tedy za činnost nenaplňující znaky provozování, nebude zpravidla považována taková „jednorázová“ činnost, kterou může vykonávat jen určitý specifický dodavatel (např. servis může být na základě jednorázových objednávek exkluzivně poskytován pouze jedním dodavatelem, obvykle výhradním zástupcem či autorem, softwaru).

provádí osoba odlišná od vydavatele aktualizace (správce, jiný dodavatel)[2], nepůjde v případě tohoto „vydavatele“ o zajišťování technických a programových prostředků ve smyslu zákona o kybernetické bezpečnosti.

Při rozboru definice provozovatele systému je potřeba se zaměřit zejména na sousloví **„technických a programových prostředků“.** Sousloví „technických a programových prostředků“ v zákoně představuje jeden pojem, a tedy postačuje, aby provozovatel systému zajišťoval buď pouze technické prostředky, nebo pouze programové prostředky, případně jejich kombinaci. **Jinými slovy, provozovatelem systému je orgán nebo osoba, která pro správce systému** (dále také jen „správce“) **zajišťuje funkčnost systému** (nebo jeho části) **v určité požadované kvalitě, úrovni bezpečnosti a rozsahu** (tj. odpovídá za funkčnost hardware nebo software systém tvořící, například prostřednictvím smlouvy o zajištění určité úrovně podpory).

Poslední náležitostí této definice je, že se jedná o zajištění funkčnosti technických a programových prostředků **„tvořících informační nebo komunikační systém“. Institut provozovatele systému se tedy aplikuje pouze vůči zajišťování funkčnosti technických a programových prostředků tvořících informační nebo komunikační systém** (nebo jeho část) **– tedy vůči technickému vybavení, komunikačním prostředkům a programovému vybavení, které jsou daným systémem.**

Dále je potřeba podotknout, že **provozovateli systému budou nejen ty subjekty, které zajišťují funkčnost technických a programových prostředků systému jako celku, ale i ty, které zajišťují i funkčnost jen některých těchto prostředků.** Často zajišťuje funkčnost technických a programových prostředků tvořících konkrétní systém i více provozovatelů současně.

Současně je potřeba zmínit, že za provozovatele systému ve smyslu zákona o kybernetické bezpečnosti nepovažuje Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) **dodavatele provozovatelů** (tedy poddodavatele).

1.2 Obecné příklady

Níže jsou uvedeny činnosti, které lze standardně považovat za zajišťování funkčnosti technických a programových prostředků. **Vždy je ale potřeba mít na paměti, že aby se v případě subjektu provádějícího níže uvedené činnosti jednalo o provozovatele systému,**

[2] Pokud není instalace aktualizací službou nezbytně spojenou s poskytováním služby dodavatelem a správce (resp. osoba odlišná od vydavatele aktualizace) musí tuto službu (stahování a instalaci aktualizací) aktivně obstarat, resp. povolit, přebírá tím správce *de facto* úlohu implementátora aktualizace, a tedy i zajišťovatele funkčnosti programových prostředků tvořících systém. Stejná logika pak bude aplikovatelná také na případné dodavatele, kteří pro správce zajišťují provoz systému tím, že implementují aktualizace, které byly jiným subjektem vydány.

musí být vždy v konkrétním případě naplněny také všechny ostatní znaky definice provozovatele systému.

Zajišťováním funkčnosti technických a programových prostředků je možno rozumět především provádění některých bezpečnostních opatření a činností jako:

- nasazování nových aplikací a patchů do produkčního prostředí,
- nasazování hardwaru do produkčního prostředí,
- provádění konfigurace, provozu, údržby, profylaxe nebo oprav technického vybavení, komunikačních prostředků nebo programového vybavení daného systému,
- správa privilegovaných (administrátorských) a uživatelských účtů,
- poskytování cloudových služeb,
- trvalá správa auditních logů.

Provozovatelem systému podle zákona **naopak zpravidla nebude** orgán nebo osoba, která:

- určitým způsobem sice ovlivňuje fungování určeného systému, nicméně její činnost nepředstavuje zajišťování funkčnosti technických a programových prostředků tvořících systém (např. provádí hodnocení rizik, zajišťuje školení pro uživatele a administrátory apod.),
- zajišťuje funkčnost technických a programových prostředků, které ale netvoří určený systém (provozovaná aktiva jsou např. mimo rozsah systému řízení bezpečnosti informací),
- nezajišťuje funkčnost technických a programových prostředků, ale pouze tyto prostředky systému využívá (typicky uživatel),
- je dodavatelem provozovatelů (tedy poddodavatel),
- je dodavatelem programových prostředků, které mohou být v systému instalovány, ale sama je do systému nemůže implementovat, nemůže je sama v systému udržovat ani aktualizovat – tedy nezajišťuje funkčnost programových prostředků svým přímým působením v systému (např. dodavatelé operačních systémů, firmwarů i aplikačního softwaru bez možnosti přístupu k systému),
- zajišťuje provoz či testování technických a programových prostředků v testovacím nebo vývojovém prostředí, a tato prostředí jsou od produkčního prostředí určeného systému oddělena (např. testování zranitelností před nasazením do produkčního prostředí).

Všechny výše uvedené příklady dodavatelů, kteří nejsou provozovatelem systému podle zákona, samozřejmě platí pouze v případě, že jsou v rámci příkladu zváženy všechny náležitosti definice provozovatele systému a takový dodavatel tuto definici nenaplní.

Obecné příklady jsou pouze výběrem nejčastějších případů a rozhodně se nejedná o konečný výčet. Stěžejním je vždy naplnění zákonné definice.

1.3 Specifické situace známé z praxe

Na tomto místě je vhodné uvést také specifické případy, se kterými se NÚKIB ve vztahu k institutu provozovatele systému setkal a považuje za vhodné je zde výslovně uvést.

Stejně tak jako v případech uvedených výše, i zde samozřejmě stále platí, že u níže uvedených příkladů je potřeba mít na paměti definici provozovatele systému.

Security Operations Centre (SOC)

Pokud povaha činnosti dodavatele SOC spočívá pouze ve vyhodnocování kybernetických bezpečnostních událostí a incidentů, přičemž tento dodavatel přímo neprovádí žádné činnosti v systému, pak provozovatelem systému nebude. Naopak, pokud může dodavatel aktivně zasahovat do technických a programových prostředků určeného systému, pak provozovatelem systému bude (v takovém případě bude součástí určeného systému také technické vybavení, komunikační prostředky a programové vybavení SOC týmu, tedy ty technické a programové prostředky dohledového systému, které zasahují do určeného systému).

Adresářové služby

Z praktického pohledu může mít adresářová služba v závislosti na organizační struktuře a systémové architektuře společnosti několik vzájemně provázaných úrovní: koncernová adresářová služba, adresářová služba konkrétní společnosti, adresářová služba technologické sítě nebo samostatná adresářová služba určeného systému. Provozovatelem systému bude dodavatel té úrovně adresářové služby, na které se uživatelé určeného systému autentizují (přičemž tato adresářová služba je součástí určeného systému).

Dodavatel bezpečnostních řešení

Pokud se bude jednat pouze o dodávky služeb spočívajících v konzultantské nebo poradenské činnosti, nebude se jednat o provozovatele systému. Pokud se však bude jednat o dodávky spojené se zajišťováním funkčnosti hardware nebo software, pak se o provozovatele systému jednat bude.

Vývoj programového vybavení

Ačkoli má být vývoj primárně prováděn ve vývojovém prostředí, testován v testovacím prostředí a teprve poté nasazen do produkčního prostředí, lze se v praxi výjimečně setkat i s případy, kdy je vývoj nutno prováděn přímo v produkčním prostředí (např. v případech, kdy fyzické prostředí, které je produkčním prostředím řízeno, nelze v testovacím prostředí nasimulovat). V takovém případě bude i vývoj spadat pod zajišťování technických a programových prostředků tvořících informační systém.

Bezpečnostní role

Pokud mají bezpečnostní role, zejm. architekt kybernetické bezpečnosti, garant (zejm. podpůrného) aktiva nebo manažer kybernetické bezpečnosti, které jsou zajišťovány externě (tzn. nikoli na základě pracovněprávního vztahu), možnost zasahovat[3] do technických nebo programových prostředků, které tvoří určený informační nebo komunikační systém, bude jejich činnost naplňovat znaky provozování. V případě, že možnost zasahovat do technických nebo programových prostředků mít nebudou – nebude se v takovém případě jednat o provozovatele.

Smyslem této kapitoly je vysvětlit jednotlivé definiční znaky institutu provozovatele systému podle § 2 písm. g) zákona o kybernetické bezpečnosti, zasadit je do kontextu a uvést některé příklady jejich naplnění a nenaplnění.

Jakmile dojde u subjektu (dodavatele) k naplněné těchto definičních znaků, stává se ze zákona provozovatelem systému.

Pro správnou praktickou aplikaci tohoto institutu a řádný výkon činnosti provozovatele je však potřeba takového provozovatele systému ze strany správce řádně identifikovat.

[3] Zásahem se rozumí např. tvorba účtů, nastavování adresářových služeb, nastavování pravidel na firewallech, obecně tedy nikoli pouhý návrh architektury sítě, hodnocení aktiv nebo tvorba bezpečnostní dokumentace, ale vlastní realizace technických bezpečnostních opatření.

2 Identifikace provozovatele systému

2.1 Vztah mezi správcem a provozovatelem systému z pohledu identifikace

Identifikací provozovatele je nutno chápat proces vyhledání dodavatelů, kteří definici provozovatele naplňují, a to za účelem jejich informování o tom, že se stali povinnými osobami podle zákona o kybernetické bezpečnosti. S ohledem na znění zákona a výše uvedené nelze identifikací rozumět „určení“ osoby zajišťující funkčnost technických a programových prostředků informačního nebo komunikačního systému – provozovatelem se dodavatel stává ze zákona naplněním definičních znaků, správce tedy neprovádí žádné určení, ani nevybírá na základě své vůle, který dodavatel provozovatelem bude a který ne.

Správce systému je, na rozdíl od svých dodavatelů, tím, kdo má vždy jako jediný možnost objektivně a informovaně porovnat zákonnou definici provozovatele systému podle § 2 písm. g) zákona s činnostmi svých dodavatelů a takové dodavatele, kteří tuto definici naplňují, pak identifikovat provozovateli systému.

Dodavatelé bez zapojení správce nemohou mít vždy s jistotou dostatek informací k tomu, aby sami posoudili, např. zda jimi poskytované dodávky jsou činěny v rámci technických a programových prostředků systému spadajícího pod zákon o kybernetické bezpečnosti, anebo zda činnost, kterou vůči takto určenému systému vykonávají, představuje zajišťování funkčnosti technických a programových prostředků tvořících systém ve smyslu zákona, a tedy **zda jsou provozovatelem systému podle tohoto zákona.**

Ve věci identifikace provozovatele systému (zejména pro notifikační povinnost správce vůči provozovateli) je hlavní odpovědnost na správci. Právě správce totiž (ať už na základě právní zásady „co není zákonem zakázáno, je dovoleno“, nebo také výslovně v souladu s § 6a odst. 1 zákona[4]), pověřuje jiný orgán nebo osobu provozováním systému, a jedině správce má dostatek informací a znalostí, aby mohl identifikovat provozovatele systému naplňujícího výše uvedenou definici.

Je to právě správce, kdo disponuje informacemi o tom, co je určeným systémem spadajícím do působnosti zákona o kybernetické bezpečnosti, z čeho je tvořen, zda jej provozuje jeden či více dodavatelů, jak jsou rozděleny role jednotlivých dodavatelů, a s ohledem na tyto

[4] S institutem provozovatele systému souvisí § 6a odst. 1 zákona, který se však vztahuje pouze na informační a komunikační systém kritické informační infrastruktury nebo na významný informační systém. Z tohoto důvodu jej nelze aplikovat ve vztahu mezi provozovatelem základní služby a správcem nebo provozovatelem informačního systému základní služby. Uvedené však rozhodně neznamená, že by správce informačního systému základní služby nebyl oprávněn provozování systému zcela nebo z části outsourcovat (pokud mu to jiný zákon nezakazuje). Oprávnění pověřit provozováním informačního systému základní služby jiný subjekt za předpokladu, že to není jiným právním předpisem výslovně vyloučeno, plyne z dalších právních předpisů (zejm. zákona č. 89/2012 Sb., občanský zákoník nebo zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích), resp. ze zásady smluvní volnosti.

znalosti pak především, zda určitým dodavatelem poskytovaná činnost skutečně spočívá v zajišťování funkčnosti technických a programových prostředků tvořících systém.

Dodavatel, který byl správcem informován o tom, že naplňuje definici provozovatele, avšak tuto definici objektivně nenaplňuje, není provozovatelem systému. Pokud však dodavatel zákonnou definici provozovatele objektivně naplňuje, správce jej o této skutečnosti informoval, avšak dodavatel se za provozovatele z nějakého důvodu nepovažuje a s informováním ze strany správce nesouhlasí, dostává se svou případnou nečinností do rozporu se zákonem z důvodu neplnění svých povinností provozovatele systému.

2.2 Identifikace provozovatele systému – obecný model

Obecný model procesu identifikace provozovatele plyne z § 8 vyhlášky o kybernetické bezpečnosti, konkrétně z odst. 1 písm. c) a odst. 3 písm. d) tohoto ustanovení.

Zmíněná ustanovení konkretizují povinnost správce v rámci řízení dodavatelů[5], a to na prokazatelné písemné informování svých významných dodavatelů[6], přičemž náležitostí prokazatelného informování je mj. též vyrozumění o skutečnosti, že významný dodavatel je zároveň provozovatelem.[7]

Informování může být provedeno dokumentem, v rámci kterého dochází k informování o vedení dodavatele v evidenci významných dodavatelů[8], může být součástí pověření provozováním[9], seznámení dodavatelů s pravidly pro dodavatele, pokud jsou určeny pro konkrétního dodavatele[10], nebo může být provedeno jiným dokumentem. **Ve všech případech by však mělo být provedeno prokazatelně, adresně a ve vztahu ke každému jednotlivému provozovateli samostatně. Podstatnými náležitostmi prokazatelnosti bude informace o tom, že se jedná o provozovatele konkrétního systému podle zákona o kybernetické**

[5] Zákonný základ této povinnosti pramení z § 4 odst. 2 a § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti.
[6] Podle § 2 písm. n) vyhlášky o kybernetické bezpečnosti se významným dodavatelem rozumí „**provozovatel informačního nebo komunikačního systému** a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému“.
[7] Informování podle § 8 odst. 1 písm. c) vyhlášky o kybernetické bezpečnosti obsahuje především informaci o tom, že je konkrétní významný dodavatel veden v evidenci významných dodavatelů podle § 8 odst. 1 písm. b) vyhlášky o kybernetické bezpečnosti.
[8] Podle § 8 odst. 1 písm. c) vyhlášky o kybernetické bezpečnosti.
[9] Zde je vhodné podotknout, že už z podstaty oprávněnosti správce informačního nebo komunikačního systému kritické informační infrastruktury nebo správce významného informačního systému pověřit určitého dodavatele provozem podle § 6a odst. 1 zákona o kybernetické bezpečnosti je potřeba dovodit také určitou notifikační povinnost. Náležitosti pověření zákon o kybernetické bezpečnosti sice neupravuje, nicméně správce tím, že pověří provozováním systému jiný subjekt, fakticky rozšiřuje okruh osob odpovědných za soulad tohoto systému se zákonem o kybernetické bezpečnosti o provozovatele systému. Z toho důvodu je prakticky nezbytné, aby pověření bylo učiněno takovým způsobem, aby byl správce vždy schopen prokázat jeho existenci, a aby součástí pověření (byť i ve formě samostatného dokumentu) bylo i informování dodavatele o tom, že se stává provozovatelem podle zákona o kybernetické bezpečnosti.
[10] Podle § 8 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti.

bezpečnosti, s čímž je neodmyslitelně spjato také stanovení systému spadajícího do působnosti zákona o kybernetické bezpečnosti, vymezení technických a programových prostředků, které tvoří určený systém, resp. vymezení činností dodavatele v rámci určeného systému, a to tak, aby došlo k dostatečné identifikaci toho, pro co se dodavatel stává provozovatelem daného systému.

Povinnost obsažená v § 8 odst. 1 písm. c) a odst. 3 písm. d) vyhlášky o kybernetické bezpečnosti se uplatní obecně, tedy nejen na správce informačního nebo komunikačního systému kritické informační infrastruktury nebo správce významného informačního systému, ale také na správce informačního systému základní služby.

Z pohledu povinnosti informovat provozovatele není podstatné, zda provoz systému je správcem plně outsourcován k dodavateli nebo dodavatelům, nebo je provoz systému správcem systému zajišťován částečně, přičemž zbývající části zajišťuje dodavatel nebo dodavatelé. Správce má povinnost informovat dodavatele o tom, že je provozovatelem systému v obou těchto případech.

Nesplněním povinnosti vyplývající z § 8 vyhlášky o kybernetické bezpečnosti se pak správce dostává do rozporu se zákonnou povinností řídit své dodavatele [bezpečnostní opatření podle § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti], za což mu může být uložena pokuta až ve výši 5 000 000 Kč.

Informování je ze své podstaty jednostranný právní akt učiněný správcem systému. Informování je však nutno důsledně odlišovat od procesu smluvního zajištění zavádění a provádění bezpečnostních opatření a vymezení práv a povinností mezi správcem a provozovatelem systému (viz dále).

Návrh možného znění identifikování provozovatele formou dokumentu, v rámci kterého dochází k informování o vedení dodavatele v evidenci významných dodavatelů a o skutečnosti, že je současně provozovatelem systému, je přílohou tohoto dokumentu.

2.3 Identifikace provozovatele systému – speciality identifikace provozovatele systému v rámci jednotlivých modelů provozu systému

2.3.1 Správce prvku kritické informační infrastruktury a významného informačního systému neprovozuje svůj systém – provoz je plně outsourcován k dodavateli nebo dodavatelům

Nad rámec výše uvedeného zákon o kybernetické bezpečnosti v § 4a odst. 1 stanoví, že správce informačního nebo komunikačního systému kritické informační infrastruktury nebo správce významného informačního systému, který není provozovatelem systému (tedy nezajišťuje funkčnost technických a programových prostředků), je povinen neprodleně a prokazatelně informovat provozovatele [dodavatele naplňujícího zákonnou definici podle

§ 2 písm. g) zákona] systému o tom, že tento definici naplňuje a je tedy povinnou osobou podle příslušného písmene § 3 zákona.

Nesplnění povinnosti řádně a včas informovat provozovatele podle § 4a odst. 1 zákona může být sankcionováno pokutou až ve výši 1 000 000 Kč. Současně s tím se nesplněním povinnosti vyplývající z § 8 vyhlášky o kybernetické bezpečnosti správce dostává i do rozporu se zákonnou povinností řídit své dodavatele [bezpečnostní opatření podle § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti], za což mu může být uložena pokuta až ve výši 5 000 000 Kč.

Řádným informováním provozovatele systému dojde jednak ke splnění povinnosti podle § 8 vyhlášky o kybernetické bezpečnosti, jednak ke splnění povinnosti vyplývající z § 4a odst. 1 zákona (v rámci aktuální právní úpravy se jedná o duplicitní povinnost).

2.3.2 Správce provozuje systém plně sám

Pokud je správce zároveň provozovatelem svého systému, informační povinnost se na tuto situaci z podstaty věci neuplatní.

2.3.3 Provozovatel informačního systému základní služby, v případech, kdy provozovatel základní služby je rozdílný od správce nebo provozovatele informačního systému základní služby

Zákon v § 4a odst. 3 upravuje specifickou situaci, kdy provozovatel základní služby, který není správcem ani provozovatelem svých informačních systémů základní služby, je povinen správce nebo provozovatele svého informačního systému základní služby neprodleně a prokazatelně informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f) zákona. Provozovatelů systému může být u jednoho systému více, v případě správce systému půjde ve vztahu k jednomu konkrétnímu systému o jednu osobu.

Ze znění § 4a odst. 3 zákona o kybernetické bezpečnosti je zřejmé, že se toto ustanovení vztahuje **pouze** na případy, kdy provozovatel základní služby není zároveň ani správce, ani provozovatel systému (zde informačního systému základní služby).

Ustanovení § 4a odst. 3 zákona o kybernetické bezpečnosti je především nutno chápat v kontextu § 3 písm. g) zákona, který uvádí, že orgánem nebo osobou je „provozovatel základní služby, *pokud není správcem nebo provozovatelem podle písmene f)*“. Pokud je určitý subjekt určen jako provozovatel základní služby, avšak naplňuje zároveň buď definici správce systému [§ 2 písm. e) zákona], nebo definici provozovatele systému [§ 2 písm. g) zákona], případně obou, není k němu již z pohledu zákona přistupováno jako k provozovateli základní služby podle § 3 písm. g) zákona, ale jako ke správci, případně provozovateli, informačního systému základní služby podle § 3 písm. f) zákona.

Zmíněné ustanovení § 4a odst. 3 zákona o kybernetické bezpečnosti se tedy vztahuje pouze na takové provozovatele základní služby, kteří jsou pouze orgánem nebo osobou podle § 3 písm. g) zákona. Takový provozovatel základní služby je povinen neprodleně informovat správce informačního systému základní služby, stejně tak jako provozovatele informačního systému základní služby, když je mu takový znám.

Jakmile je správce informačního systému základní služby informován podle § 4a odst. 3 zákona o kybernetické bezpečnosti, uplatní se na něj všechny povinnosti identifikace a informování provozovatele ze zákona a vyhlášky o kybernetické bezpečnosti, jak jsou popsány výše.

Pro všechny výše uvedené specifické modely provozu systému tedy platí, že ať už existuje obecná povinnost pro všechny správce systému daná § 8 vyhlášky o kybernetické bezpečnosti, nebo zákon o kybernetické bezpečnosti tuto oblast upravuje pro správce vybraných systémů speciálně, je povinností správce informačního systému vyhledat všechny dodavatele, kteří zajišťují funkčnost technických a programových prostředků tvořících daný systém, a informovat je o tom, že naplňují zákonnou definici provozovatele systému.

3 Provozovatel systému a plnění povinností

3.1 Povinnosti provozovatele systému obecně

V případě, že byl provozovatel systému správcem informován, je povinen plnit povinnosti podle zákona o kybernetické bezpečnosti.

V rámci plnění povinností se bude jednat především o povinnosti:

- hlásit kontaktní údaje NÚKIB (§ 16 zákona),
- zavádět bezpečnostní opatření (§ 4 zákona),
- hlásit kybernetické bezpečnostní incidenty (§ 8 zákona),
- provádět opatření (§ 11 zákona),

stejně tak jako o další povinnosti, kterými jsou např. povinnost předat správci data, provozní údaje a informace na vyžádání (§ 6a odst. 2 zákona), povinnost předat správci data, provozní údaje a informace při ukončení spolupráce (§ 6a odst. 3 zákona), povinnost předat správci data, provozní údaje a informace na základě rozhodnutí vydaného NÚKIB (§ 15a zákona).

Díky informování ze strany správce systému, které obsahuje výše uvedené náležitosti, tedy bude obsahovat informaci o tom, že se jedná o provozovatele systému podle zákona o kybernetické bezpečnosti a vymezení rozsahu systému a činností, pro které se stává dodavatel provozovatelem, **má provozovatel systému dostatek informací pro plnění těchto povinností.**

V případě, že byl provozovatel systému správcem informován, ale nemá dostatek informací k provádění některé z těchto povinností (např. v důsledku toho, že informování ze strany správce bylo neúplné), **je jeho povinností vynaložit veškeré úsilí, které je možno požadovat[11], k doplnění těchto informací.**

3.2 Povinnost zavádět bezpečnostní opatření

Zvláštní pozornost je potřeba věnovat povinnosti zavádět bezpečnostní opatření. Při zavádění a provádění bezpečnostních opatření podle zákona o kybernetické bezpečnosti je potřeba mít vždy na paměti, že podle § 4 odst. 2 zákona mají povinné osoby (tedy správce a provozovatel systému) zavést bezpečnostní opatření v takovém rozsahu, který je nezbytný pro zajištění kybernetické bezpečnosti informačního nebo komunikačního systému. Bezpečnostní opatření je tedy potřeba realizovat právě s ohledem na toto ustanovení (kdy primárním cílem je

[11] Především z důvodu § 21 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

zabezpečení systému, nikoli duplicitní zavádění bezpečnostních opatření na straně správce i provozovatele tam, kde to není smysluplné a zákon ani vyhláška to výslovně nevyžadují).

Správce systému, tedy ten, kdo určuje jeho účel a podmínky jeho provozování, je v postavení toho, kdo má mít všechny informace o tom, jaká konkrétní bezpečnostní opatření mají být ve vztahu k systému ze strany provozovatele systému zavedena, neboť pouze správce systému má dostatek informací k tomu, aby mohl bezpečnostní požadavky definovat (a to i kdyby měl podstatnou část informací nezbytných pro výběr bezpečnostních opatření získat od provozovatele), **a vždy nese odpovědnost za jejich realizaci.**

Provozovatel systému bude zavádět bezpečnostní opatření typicky tam, kde je není schopen zavést správce, což vyplývá z cílů zákona i z podstaty zavedení institutu provozovatele systému, **avšak bude tak činit na základě řízení správcem – v takových případech budou za zavádění a provádění bezpečnostních opatření odpovědni jak správce, tak provozovatel.** Nemělo by tedy docházet k tomu, že provozovatel systému sám ze své inciativy a bez předchozí konzultace a schválení správcem začne zavádět bezpečnostní opatření nad rámec rozsahu, který vyplývá ze smluvního plnění.

Řízení provozovatele správcem má svá pravidla daná především § 8 a přílohou č. 7 vyhlášky o kybernetické bezpečnosti. **Správce systému v souvislosti s řízením rizik spojených s provozovateli systému zajistí, aby smlouvy uzavírané s provozovateli systému obsahovaly relevantní oblasti uvedené v příloze č. 7 vyhlášky o kybernetické bezpečnosti, a pravidelně přezkoumává plnění těchto smluv z hlediska systému řízení bezpečnosti informací.[12] Správce musí v rámci uzavíraných smluvních vztahů s provozovatelem zajistit především to, aby byly stanoveny způsoby a úrovně realizace bezpečnostních opatření, a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.[13] Stejně tak jsou správci povinni zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou.[14]**

Provozovatel systému realizuje bezpečnostní opatření – realizace musí probíhat prostřednictvím daných způsobů a úrovní realizace. Odpovědností provozovatele systému bude v takové situaci typicky to, aby byla realizace na dané úrovni, odpovědností správce systému typicky kontrola toho, zda jsou bezpečnostní opatření skutečně realizována tak, jak bylo dohodnuto.

[12] Podle § 8 odst. 1 písm. f) a g) vyhlášky o kybernetické bezpečnosti.
[13] Podle § 8 odst. 2 písm. b) vyhlášky o kybernetické bezpečnosti.
[14] Podle § 4 odst. 4 zákona o kybernetické bezpečnosti.

Ve výsledku je tedy nutné dosáhnout toho, aby bylo v rámci vzájemného vztahu správce a provozovatele systému jasně a v přiměřených a vhodných podrobnostech stanoveno, které povinnosti spojené se zaváděním a prováděním bezpečnostních opatření vykonává správce a které provozovatel. **Obecný požadavek, že dodavatel má provádět všechny činnosti v souladu se zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, je nedostatečný.** V případě, že nebudou smluvní povinnosti provozovatele stanoveny dostatečně konkrétně, může nastat situace, že provozovatel ve snaze dosáhnout splnění všech požadavků zavede a bude provádět bezpečnostní opatření, která nebudou pro daný systém vhodná či budou duplikovat již realizovaná bezpečnostní opatření na straně správce systému – takto vzniklá situace je v rozporu s účelem zákona o kybernetické bezpečnosti i povinnostmi správce podle § 8 odst. 2 písm. b) vyhlášky o kybernetické bezpečnosti a správce by ji vůbec neměl dopustit. Stejně tak může dojít k tomu, že nebude dosaženo zavedení a provedení bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti určeného systému, což by správce ani provozovatel neměli nikdy dopustit.

3.3 Úhrada nákladů provozovateli systému

Otázka náhrady finančních prostředků (vynaložených nákladů) **za zavádění a provádění bezpečnostních opatření, či za plnění jiných povinností v rámci vztahu správce – provozovatel, není zákonem o kybernetické bezpečnosti nijak regulována, konkrétní podoba dohody správce s provozovatelem ohledně úhrady nákladů je tedy věcí smluvní volnosti** (s případnými specifiky vyplývajícími z jiného právního předpisu).

3.4 Přechodné ustanovení zavedené zákonem č. 104/2017 Sb.

Přechodným ustanovením zákona č. 104/2017 Sb. byla nově definovaným povinným osobám – provozovatelům systémů – poskytnuta lhůta pro zavedení bezpečnostních opatření a stanovena povinnost správců uhradit náklady spojené s jejich zavedením.

Toto ustanovení vstoupilo v účinnost dne 1. července 2017 a nejdelší daná lhůta (6 měsíců ode dne nabytí účinnosti novely pro zavedení bezpečnostních opatření) uplynula 1. ledna 2018. **Toto přechodné ustanovení se tedy v současné době již nepoužije** (lhůty již uplynuly) **a navíc jej není možné aplikovat na vztahy vzniklé po nabytí účinnosti zákona č. 104/2017 Sb.**

Toto přechodné ustanovení také stanovilo, že „v případě zavedení bezpečnostních opatření má provozovatel nárok na úhradu nákladů spojených s přijetím bezpečnostního opatření; náklady provozovateli uhradí správce daného systému“. Jak vyplývá z informací uvedených výše, v tuto chvíli se již toto ustanovení nepoužije a vztah mezi správcem a provozovatelem je ovládán smluvní volností a dohoda o úhradě přiměřených nákladů tedy není obligatorním požadavkem zákona o kybernetické bezpečnosti.

3.5 Vztah provozovatele systému a institutu významného dodavatele podle § 2 písm. n) vyhlášky o kybernetické bezpečnosti

Dle definice je významným dodavatelem provozovatel informačního nebo komunikačního systému a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému.

Z této definice tedy vyplývá, že po zhodnocení všech dodavatelů a případné identifikaci některých jako provozovatelů systému podle pravidel uvedených v tomto dokumentu je potřeba zhodnotit zbylé dodavatele také z toho pohledu, zda s povinnou osobou vstupují do právního vztahu, který je významný z hlediska bezpečnosti určeného systému. V tomto případě je především potřeba věnovat velkou pozornost těm dodavatelům, kteří mají vztah k aktivům v rozsahu systému řízení bezpečnosti informací a nebyli identifikováni jako provozovatelé systému.

Vliv na bezpečnost určeného systému mohou mít i ostatní dodavatelé, pokud se tak stane, mělo by dojít ke zvážení rozšíření rozsahu systému řízení bezpečnosti informací i o tohoto dodavatele.

3.6 Provozovatel více různých systémů regulovaných zákonem

V případě, že určitý dodavatel naplní definici provozovatele systému pro více různých systémů (typicky např. v případě telekomunikační infrastruktury, cloudových služeb apod.), je nutno na takového dodavatele pohlížet vždy jako na provozovatele konkrétního řešeného systému. Zjednodušeně řečeno tedy bude takový dodavatel v pozici samostatného provozovatele vůči několika různým určeným systémům a jako takový bude muset být např. informován každým správcem každého určeného systému a své povinnosti bude plnit vždy s ohledem na konkrétní systém, který provozuje.

Stejně tak je potřeba mít na paměti také to, že v případě, že bude celý systém výše zmíněného dodavatele určen jako systém spadající pod zákon o kybernetické bezpečnosti, vystupuje sice tento dodavatel vůči svému systému jako správce, ale vůči ostatním správcům je stále provozovatelem jejich části systému (příkladem mohou být např. mobilní operátoři, kteří jsou současně správci svého komunikačního systému, avšak zároveň služby jejich komunikačního systému slouží k zajištění komunikací jiných, např. bankovních systémů, systémů státní správy, či systémů zajišťujících řídicí systémy energetických sítí – pro ně budou stále v pozici provozovatele těchto systémů).

4 Povinnost řídit dodavatele

Krom provozovatele systému a významného dodavatele se bude povinná osoba podle zákona o kybernetické bezpečnosti v praxi setkávat i s „ostatními“ dodavateli, tedy zbytkovou kategorií osob, které s povinnou osobou vstupují do právního vztahu, který není významný z hlediska bezpečnosti informačního a komunikačního systému.

Povinná osoba má povinnost řídit všechny své dodavatele, tedy nejen provozovatele a významné dodavatele, a to v souladu s § 8 vyhlášky o kybernetické bezpečnosti. Základní povinností v rámci řízení dodavatelů je řídit rizika spojená se všemi typy dodavatelů. Další povinností týkající se všech typů dodavatelů je povinnost jejich seznámení s pravidly pro dodavatele, které stanoví povinná osoba.

Ve spojení s významným dodavatelem (tzn. jak provozovatelem systému, tak s každým, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti systému) má povinná osoba povinnost vést evidenci významných dodavatelů[15], povinnost významné dodavatele prokazatelně písemně informovat o jejich vedení v této evidenci[16] (přičemž jedním ze způsobů splnění této povinnosti je informování významného dodavatele s pomocí níže uvedeného vzoru), a další povinnosti uložené v rámci § 8 vyhlášky o kybernetické bezpečnosti. Jednou z nejvýznamnějších povinností je pak povinnost u významných dodavatelů v rámci uzavíraných smluvních vztahů stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření[17]. Další povinnosti vztahující se k provozovateli systému jsou dány také zákonem o kybernetické bezpečnosti.

Vyhláška o kybernetické bezpečnosti výslovně požaduje, aby v informování dodavatele bylo výslovně uvedeno vyrozumění o skutečnosti, že dodavatel je pro povinnou osobu významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem.[18] „Ostatní“ dodavatele naopak není potřeba o jejich „postavení“ nijak specificky informovat.

Níže uvedené vzory informování slouží pouze jako pomůcka pro povinné osoby. Jejich smyslem je upozornit na hlavní body, které musí být v rámci informování uvedeny, aby byl naplněn smysl a účel tohoto informování. V praxi může informování obsahovat také další informace. Jak je již zmíněno výše, informování významného dodavatele vychází z § 8 odst. 1 písm. b) a c) vyhlášky o kybernetické bezpečnosti, jeho náležitosti jsou pak dány ustanovením § 8 odst. 3 této vyhlášky a dále upřesněny podkapitolou 2.2 tohoto dokumentu.

[15] § 8 odst. 1 písm. b) vyhlášky o kybernetické bezpečnosti
[16] § 8 odst. 1 písm. c) vyhlášky o kybernetické bezpečnosti
[17] § 8 odst. 2 písm. b) vyhlášky o kybernetické bezpečnosti
[18] § 8 odst. 3 písm. d) vyhlášky o kybernetické bezpečnosti

5 Příloha – vzory informování dodavatele

5.1 Vzor informování dodavatele o tom, že je významným dodavatelem a současně provozovatelem systému

Vážení,

tímto Vás informujeme, že podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, naplňuje Vaše organizace *[název dodavatele]*, sídlem *[sídlo dodavatele]*, IČO *[IČO dodavatele]*, definici provozovatele systému ve smyslu § 2 písm. g) zákona o kybernetické bezpečnosti, a je tedy významným dodavatelem podle § 2 odst. n) vyhlášky o kybernetické bezpečnosti, a jako takového Vás vedeme v naší evidenci významných dodavatelů. Naplnění této definice plyne z toho, že jste na základě *[označení smlouvy nebo jiného právního aktu s dodavatelem]*, jejímž předmětem je *[základní popis pro zpřesnění identifikace smlouvy nebo jiného právního aktu]*, s naší organizací v právním vztahu, v rámci kterého zajišťujete funkčnost technických a programových prostředků našeho systému *[bližší identifikace systému]*, přičemž tento je *[zvolit správné označení: kritickou informační infrastrukturou, významným informačním systémem, nebo informačním systémem základní služby]* podle zákona o kybernetické bezpečnosti. Naše organizace je správcem tohoto systému podle zákona o kybernetické bezpečnosti.

Konkrétně výše zmíněnou definici provozovatele systému vůči systému naší organizace naplňujete z toho důvodu, že dodáváte *[dostatečně konkrétní vymezení technických a programových prostředků nebo jiného plnění, které tvoří dodávky tohoto dodavatele, resp. vymezení činností dodavatele v rámci systému, pro které je jeho postavení významné z hlediska bezpečnosti systému]*.

Přílohou tohoto informování je také v souladu § 8 odst. 1 písm. a) vyhlášky obsah pravidel pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací naší organizace, přičemž Vaše postavení jakožto významného dodavatele pro Vás přináší i zvláštní režim v rámci těchto pravidel. *[Přílohou tohoto informování jsou pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací podle § 8 odst. 1 písm. a) a d) vyhlášky o kybernetické bezpečnosti].*

5.2 Vzor informování dodavatele systému o tom, že je významným dodavatelem

Vážení,

tímto Vás informujeme, že podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, naplňuje Vaše organizace *[název dodavatele]*, sídlem *[sídlo dodavatele]*, IČO *[IČO dodavatele]*, definici významného dodavatele podle § 2 odst. n) této vyhlášky, a jako takového Vás vedeme v naší evidenci významných dodavatelů. Naplnění této definice plyne z toho, že jste na základě *[označení smlouvy nebo jiného právního aktu s dodavatelem]*, jejímž předmětem je *[základní popis pro zpřesnění identifikace smlouvy nebo jiného právního aktu]*, s naší organizací v právním vztahu, který je významný z hlediska bezpečnosti našeho systému *[bližší identifikace systému]*, přičemž tento je *[zvolit správné označení: kritickou informační infrastrukturou, významným informačním systémem, nebo informačním systémem základní služby]* podle zákona o kybernetické bezpečnosti. Zároveň Vás informujeme, že Vaše organizace je ve smyslu vyhlášky o kybernetické bezpečnosti významným dodavatelem, avšak ne v rozsahu pojmu provozovatele systému ve smyslu této vyhlášky. Naše organizace je správcem tohoto systému podle zákona o kybernetické bezpečnosti.

Konkrétně výše zmíněnou definici významného dodavatele vůči systému naší organizace naplňujete z toho důvodu, že dodáváte *[dostatečně konkrétní vymezení technických a programových prostředků nebo jiného plnění, které tvoří dodávky tohoto dodavatele, resp. vymezení činností dodavatele v rámci systému, pro které je jeho postavení významné z hlediska bezpečnosti systému]*.

Přílohou tohoto informování je také v souladu § 8 odst. 1 písm. a) vyhlášky obsah pravidel pro dodavatele, které zohledňují požadavky systému řízení bezpečnosti informací naší organizace, přičemž Vaše postavení jakožto významného dodavatele pro Vás přináší i zvláštní režim v rámci těchto pravidel. *[Přílohou tohoto informování jsou pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací podle § 8 odst. 1 písm. a) a d) vyhlášky o kybernetické bezpečnosti].*

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
31. 10. 2017	1.0	Odb. RAP	Vytvoření dokumentu
12. 11. 2018	2.0	Odb. regulace	Doplnění problematiky provozovatele základní služby (doplněna nová kapitola)
28. 1. 2019	2.1	Odb. regulace	Změna kontaktních údajů
4. 3. 2020	3.0	Odb. regulace	Celková revize, doplnění poznatků z praxe, upřesnění textu na základě nejčastějších dotazů a úpravy rozložení kapitol pro celkové zpřehlednění dokumentu
10. 3. 2021	3.1	Odb. regulace	Doplnění vzorů informování významného dodavatele, doplnění obecných informací k řízení dodavatelů
22. 12. 2022	3.2	Odb. regulace	Změna kontaktních údajů