PORTÁL NÚKIB

Kybernetická bezpečnost obcí

TLP:CLEAR

6. prosince 2024

Verze 1.0

Národní úřad
pro kybernetickou
a informační bezpečnost

1 Co se dozvím v tomto dokumentu?

Proč je potřeba kybernetickou bezpečnost (neboli dále také zkráceně „KB“) řešit? K čemu je nová regulace dobrá? Co mám tedy konkrétně zabezpečit? Co všechno je výkon svěřených pravomocí? Co městská policie a městské části? Jak zavádět bezpečnostní opatření?

To jsou otázky, kterým se věnuje tento materiál. V následujících kapitolách se čtenář tohoto dokumentu dozví, jak postupovat při plnění povinností podle nového zákona o kybernetické bezpečnosti a **vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností** (dále jen „**vyhláška**“), která je relevantní právě pro obce s rozšířenou působností.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

2 Praktické přínosy nové regulace

Kromě samotného zvýšení úrovně KB v organizaci, má nový zákon o KB pro obce s rozšířenou působností další praktické přínosy:

- Přístup k dotačním programům pro zvyšování KB.
- Prevence a snižování finančních ztrát v případě incidentů.
- Jednodušší nakupování bezpečnostních technologií při zadávání veřejných zakázek.
- Metodická podpora NÚKIB a přístup do Portálu NÚKIB.
- Příležitost pro zmapování procesů v organizaci.

3 Rozsah regulované služby Výkon svěřených pravomocí

Tato kapitola se věnuje vymezení toho, kde bude a kde nebude obec zavádět dílčí bezpečnostní opatření požadovaná novým zákonem o KB a jeho prováděcími předpisy (vyhláškami).

Podle § 12 návrhu nového zákona o KB je nutné vždy tzv. **stanovit rozsah řízení KB**. Jedná se o takové vlastní vymezení „hracího pole“, ve kterém bude dále KB řešena. V rámci takto stanoveného rozsahu se pak zavádí bezpečnostní opatření, případně hlásí incidenty, pokud by měly významný dopad v tomto rozsahu.

Obec musí v rámci stanovení rozsahu stanovit, jaké informace jsou zpracovávány a jaké služby poskytovány (tzv. primární aktiva) v návaznosti na regulovanou službu, tedy „Výkon svěřených pravomocí“. Obdobně je zde také možnost vymezení vůči tomu, kde obec bezpečnostní opatření zavádět nebude, pokud daná oblast nesouvisí přímo s regulovanou službou. Jak na to?

3.1 Vycházejte z Registru práv a povinností (RPP)

V Registru práv a povinností (dále jen RPP, https://www.szrcr.cz/cs/registr-prav-a-povinnosti) jsou evidovány veškeré agendy, které daná obec vykonává. Konkrétní aktuální příklady agend lze nalézt v tomto přehledu (https://rpp-ais.egon.gov.cz/gen/agendy-detail/). Každá agenda má pak vlastní činnosti, role, služby veřejné správy a další podrobnější údaje, které nejsou v praxi zpravidla až tak důležité pro stanovení rozsahu řízení KB.

3.2 Sdružte více souvisejících agend dle RPP do primárních aktiv

V případě větších měst může jít o vyšší desítky až stovky agend, s čímž by se špatně pracovalo. Proto je lepší a jednodušší sdružit více agend do větších celků, které budou představovat primární aktiva. **Sdružené agendy by spolu měly souviset věcně, procesně, organizačně nebo technicky.**

Lze tak například sdružit veškeré agendy vykonávané Odborem životního prostředí do primárního aktiva „Životní prostředí“. Dílčí agendy v tomto primárním aktivu pak mohou být:

- Odpadové hospodářství (A1186),
- Ochrana zemědělského a půdního fondu (A1283),
- Ochrana ovzduší (A1126),
- Myslivost (A943) a tak podobně.

Neznamená to, že všechny agendy konkrétního oddělení nebo odboru musí být vždy sdruženy do jednoho primárního aktiva. Kromě organizační struktury je možné sdružit např. agendy, které jsou vykonávány prostřednictvím stejných agendových informačních systémů nebo mají velmi podobné či spojené procesy. Dobrým vodítkem při sdružování primárních aktiv jsou tedy **společné či propojené procesy a obdobné způsoby zabezpečení jednotlivých agend a jejich informačních systémů**.

3.3 Identifikujte podpůrná aktiva

Podpůrným aktivem může být např. zaměstnanec, dodavatel, hardware či software, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby. Zjednodušeně řečeno, **podpůrná aktiva jsou to, co je potřeba k výkonu agend obce** (zajištění fungování primárních aktiv, tedy jednotlivých agend či sdružení agend).

Podpůrná aktiva se evidují ve vazbě k primárním aktivům. Podpůrná aktiva je možné evidovat po skupinách dle určitého typu. Při úvodním stanovování rozsahu KB tedy nemusí být potřeba evidovat každý jednotlivý počítač, každého jednotlivého zaměstnance nebo každý jednotlivý soubor či program v počítači, pokud budete KB vůči nim ze začátku řešit stejně či obdobně.

S rostoucím povědomím o tom, co je třeba zabezpečit, se Váš rozsah bude přirozeně zpřesňovat a stávat se více podrobným. Obdobně jako u primárních aktiv je možné seskupovat tzv. **typová podpůrná aktiva,** která spolu věcně, procesně, organizačně či technicky souvisí.

3.4 Identifikujte aktiva nesouvisející s Výkonem svěřených pravomocí

V § 12 nového zákona o KB je také uveden postup umožňující vymezení se vůči tomu, kde obec nebude zavádět bezpečnostní opatření uvedená dále v tomto materiálu. V případě řádného odůvodnění je tak možné například uvést vybrané služby poskytované obcí, které nesouvisí s výkonem svěřených pravomocí a není tedy ani účelem zákona je mít tzv. v rozsahu.

Takto identifikovaná primární a podpůrná aktiva určují rozsah řízení KB, ve kterém se následně zavádí bezpečnostní opatření dle vyhlášky.

Obecný příklad:

Agenda 1	Primární aktivum	Podpůrné aktivum 1
Agenda 2		Podpůrné aktivum 2
Agenda 3		Podpůrné aktivum 3

Vycházejte z RPP, kde najdete Vámi vykonávané agendy.
- Výpis z RPP je pouze základní přehled.
- Zkontrolujte, zda evidované agendy skutečně vykonáváte.

Sdružte více souvisejících agend dle RPP do primárních aktiv.
- Sdružené agendy by spolu měly souviset věcně, procesně, organizačně nebo technicky.
- Je vhodné vycházet z organizační struktury obecního úřadu.

Identifikujte podpůrná aktiva.
- Je možné evidovat po skupinách tzv. typových podpůrných aktiv.
- Je nutné evidovat ve vztahu k primárním aktivům (co k čemu používám).

Identifikujte aktiva nesouvisející s poskytováním regulované služby.
- Je možné s řádným odůvodněním vyjmout z rozsahu aktiva nesouvisející s výkonem svěřených pravomocí.

3.5 Centrálně spravované informační systémy

Obce standardně pracují s informačními systémy, které jsou spravovány a provozovány ústředními orgány státní správy. Typicky může jít např. o základní registry, z nichž obce sice čerpají některé údaje, ale nespravují je. Obdobně používá každá obec k výkonu své působnosti Informační systém datových schránek, který však spravuje Ministerstvo vnitra, resp. provozuje Česká pošta.

Využívání těchto systémů vyplývá přímo ze zákona. Obce nemají možnost tyto systémy nepoužívat. **Nejedná se o klasicky vztah dodavatel – odběratel.** Stát s obcemi v těchto případech neuzavírá smlouvy o poskytování daného systému. Neuplatní se tedy požadavky na obsah smluv dle přílohy č. 2 návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (více o této oblasti níže). Obec v těchto případech nemusí stát evidovat jako svého významného dodavatele a jakkoli jej řídit, informovat či evidovat.

Obce jsou při používání těchto systémů v pozici uživatele. Povinnost zavádět bezpečnostní opatření ve vztahu k těmto systémům dopadá na jejich správce. Obec tedy nemá povinnost, ani možnost, zabezpečovat například Informační systém datových schránek nebo další centrální registry.

Obec však musí zavést bezpečnostní opatření, aby nedocházelo např. k neoprávněným přístupům do těchto centrálních systémů nebo k neoprávněným zásahům do údajů vedených v daném systému.

Správce systému by měl ve vztahu k takovým systémům stanovit politiku bezpečného chování uživatelů, případně další požadavky na bezpečné používání. Obce by se těmito pravidly měly řídit.

Správce systému zajišťuje zabezpečení systému jako takového. Obec zajišťuje dodržování pravidel nastavených správcem a brání neoprávněným přístupům či změnám v používaných systémech.

Má-li obec povinnost využívat určitý konkrétní státem spravovaný systém, **neuplatní se požadavky na obsah smluv s dodavateli** dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

3.6 Městské části (s výjimkou MČ hl. m. Prahy)

Území statutárních měst se podle zákona o obcích může členit na městské obvody nebo městské části s vlastními orgány samosprávy. **Městské části a obvody nejsou z pohledu práva samostatnou právnickou osobou a nemají zpravidla vlastní IČO.** Výjimkou jsou městské části hlavního města Prahy, které mají specifickou právní úpravu a mohou být samostatnými regulovanými osobami.

Městská část, resp. její obecní úřad, má vlastní personální strukturu, procesy, agendy a postupy k výkonu své působnosti. Často může využívat svou vlastní oddělenou IT infrastrukturu, specifický hardware či software, a mít tedy odlišné dodavatele oproti samotnému statutárnímu městu.

Zákon nebrání tomu, aby měla městská část stanoven vlastní **rozsah řízení kybernetické bezpečnosti**, oddělený částečně nebo úplně od samotného města. Městská část si může nastavit vlastní politiky a procesy vyžadované vyhláškou. Na druhou stranu **je možné sdílet bezpečnostní opatření**, a to jak organizační, tak technická, pokud to vyhovuje potřebám města.

> **Městské části a samotná města jsou jedním právním subjektem.** Případné rozhodnutí o uložení povinnosti nebo sankce ze strany NÚKIB se bude vždy týkat obou těchto složek.
>
> Z hlediska zavádění bezpečnostních opatření **je možné vnímat obě složky odděleně**. Každá složka si může řešit kybernetickou bezpečnost samostatně, ale není vyloučeno i centralizované řízení ze strany města.
>
> Pokud je to vhodné, je možné bezpečnostní opatření **zavádět společně, resp. je sdílet**. Městská část a město mohou mít např. sdílené zálohovací řešení nebo část IT infrastruktury, případně totožné postupy pro řešení incidentů.

3.7 Obecní policie

Obecní policie je dle zákona o obecní policii orgánem obce. Nejde tedy z pohledu práva o samostatnou právnickou osobu, městská policie nemá vlastní IČO.

Zvláště ve větších městech jde o „organizaci v organizaci“. Obecní policie má typicky vlastní personální strukturu, procesy, agendy a postupy k výkonu své působnosti. Často může využívat svou vlastní oddělenou IT infrastrukturu, specifický hardware či software, může mít tedy i odlišné dodavatele oproti obecnímu úřadu.

Zákon nijak nebrání tomu, aby měla obecní policie **vlastní rozsah kybernetické bezpečnosti**, oddělený částečně nebo úplně od zbytku obce. Pro obecní policii je možné nastavit vlastní politiky a procesy vyžadované vyhláškou. Na druhou stranu je možné sdílet bezpečnostní opatření, a to jak organizační, tak technická, pokud to vyhovuje potřebám obou „organizací“.

Obecní policie a samotná obec jsou jedním právním subjektem. Případné rozhodnutí o uložení povinnosti nebo sankce ze strany NÚKIB se bude vždy týkat obou těchto složek.

Z hlediska zavádění bezpečnostních opatření **je možné vnímat obě složky odděleně**. Každá složka si může řešit kybernetickou bezpečnost samostatně – záleží na rozhodnutí obce (zřizovatele).

Pokud je to vhodné, je možné bezpečnostní opatření **zavádět společně, resp. sdílet**. Obecní policie a obec mohou mít např. sdílené zálohovací řešení nebo část IT infrastruktury, případně totožné postupy pro řešení incidentů.

4 Základní principy zavádění bezpečnostních opatření v rozsahu

Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností vychází ze základních principů pro řízení KB, které vedou k zavádění a provádění **přiměřených bezpečnostních opatření v rozsahu** určeném dle předchozí kapitoly.

4.1 Zohlednění bezpečnostních potřeb organizace

Při prvotním uvažování nad kybernetickou bezpečností je nejdůležitější **uvědomit si, co může být ohroženo, jakou to má hodnotu a jak to přiměřeně ochránit či zabezpečit**. Případně vyhodnotit, jestli má smysl vynakládat finanční a personální zdroje daným směrem na úkor něčeho podstatnějšího (důležitějšího k zabezpečení).

Prvním krokem je vůbec zamyslet se nad tím, jaké služby a informace Vaše organizace zpracovává a poskytuje. K tomuto zamyšlení dojde již při samotném určování rozsahu dle předchozích kapitol.

Druhým krokem je zamyslet se nad těmito informacemi a službami a zvážit možná nebezpečí a dopady v případě vzniku kybernetického bezpečnostního incidentu.

Obec např. disponuje důležitými dokumenty a daty, o které by neměla přijít. Existuje reálné riziko ztráty těchto dat v případě, kdy disk počítače selže a data na něm se poškodí. Proto je vhodným bezpečnostním opatřením si udělat zálohu.

Podobným způsobem je třeba se zamyslet nad všemi důležitými službami, informacemi a podpůrnými aktivy zajišťujících jejich poskytování a přijít na způsoby, jak je ochránit. Tím zajistíte, že bezpečnostní opatření budou účinná a budou mít skutečný přínos a přidanou hodnotu.

4.2 Náklady na zavedení bezpečnostních opatření

Vstupními náklady pro zavedení bezpečnostních opatření v nižším režimu budou primárně ty spojené se zaváděním tzv. **neopominutelných bezpečnostních opatření**, která jsou nutným organizačním podkladem pro zavádění dalších bezpečnostních opatření.

Zavádění bezpečnostních opatření převážně technické povahy podle § 8 až § 10 a § 12 až § 14 vyhlášky si zpravidla vyžádá finanční náklady. Tato opatření však není potřeba zavést všechna a hned. V rámci dokumentu „Přehled bezpečnostních opatření" je možné si rozplánovat zavádění opatření s ohledem na dostupné finance. Kromě toho je samozřejmě možné využít nástroje volně dostupné nebo již dříve pořízené a používané.

4.3 Nákladová přiměřenost

Nemá smysl utrácet za špičkové bezpečnostní technologie, pokud řeší jen malou nebo nepravděpodobnou hrozbu. Cenově dostupná a efektivní bezpečnostní opatření jsou:

- Základní KB školení zaměstnanců (např. jak poznat phishingový e-mail),
- Pravidelné zálohování dat,
- Silné hesla a jejich správná správa,
- Pravidelné aktualizace softwaru.

Příklad: Nákladová přiměřenost

Pokud mám běžné městské kolo v hodnotě 5 000 Kč, nemá smysl si kupovat zámek za 10 000 Kč s alarmem a GPS sledováním. S ohledem na nebezpečí krádeže a hodnotu kola je přiměřené si koupit zámek v řádu stovek korun a kolo parkovat na místě, kde je hodně lidí a bylo by nápadné, kdyby tam někdo stříhal zámek.

Na chatu není nutné instalovat drahé kamerové systémy, alarmy a bezpečnostní dveře za desetitisíce, pokud nejdražším předmětem v celé chatě je sekačka za 10 000 Kč. Dává však smysl

Bezpečnostní opatření mají být zavedena v míře nezbytné pro zajištění kybernetické bezpečnosti tak, aby byla **účinná, ale přiměřená** vzhledem k bezpečnostním potřebám organizace, které lze v praxi odvodit zejména z např. možných dopadů incidentů.

Je důležité **nepodceňovat možné dopady incidentů a hodnotu dat** a dalších spravovaných aktiv.

Vždy je nutné zvažovat, jaký je **nejhorší možný scénář**. Ztratím-li veškerá uložená data, faktury, smlouvy a další dokumenty, jaká mi vznikne **celková škoda** (resp. náklady na obnovu)?

Základní bezpečnostní opatření **snižují pravděpodobnost incidentu o desítky procent**. I když k incidentu dojde, bude mít **menší dopady** – obnovím data ze záloh, útočník se nedostane do celé sítě atp.

zamykat přístupovou branku na zahradu nebo udržovat bezpečný plot okolo pozemku, což stojí řádově méně peněz a je to přiměřené vzhledem k hrozbě krádeže a hodnotě potenciální škody.

4.4 Neopominutelná opatření

Níže uvedená bezpečnostní opatření jsou primárně organizačního charakteru, která sama o sobě nevyžadují např. nakupování nového hardware či software a slouží jako podklad pro zavedení potřebných procesů k řízení KB. Tato opatření **musí být přiměřeně zavedena**, jelikož představují absolutní minimum v oblasti KB a jsou nutným podkladem pro následné zavádění navazujících opatření a kontinuální zlepšování.

§ 4 Systém zajišťování minimální KB

- Povinnost dodržovat princip přiměřenosti při zavádění bezpečnostních opatření, tedy nutnost zavést neopominutelná bezpečnostní opatření a u dalších vyhodnotit jejich potřebu či míru zavedení.
- Vytvoření dokumentu „Přehled bezpečnostních opatření“. Jedná se o přehledový dokument opatření z vyhlášky, která byla a nebyla zavedena, včetně případného plánu jejich zavedení. Vzorový dokument je přílohou vyhlášky.
- Určení osoby pověřené za řízení KB. Pokud osoba nedisponuje vzděláním v IT nebo KB, lze proškolit např. interního zaměstnance zdarma v e-learningu NÚKIB na osveta.nukib.gov.cz. Nejsou kladeny nároky jako na manažera KB ve vyšším režimu (časové, znalostní atd.).
- Vytvoření nezbytné a relevantní bezpečnostní politiky a dokumentace v souladu s potřebami organizace.
- Zohlednění relevantních oblastí při uzavírání smluv s dodavateli (oblasti v příloze vyhlášky pro nižší režim).
- Neopomenutí požadavků na KB při akvizici, vývoji a údržbě, např. Při nákupu HW či SW.

§ 5 Požadavky na vrcholné vedení

- Absolvování školení pro vrcholné vedení například na portálu osveta.nukib.gov.cz.
- Seznámení se s dokumentem „Přehled bezpečnostních opatření“ a zajištění zdrojů v souladu s ním.
- Podpora osoby pověřené za řízení KB a prosazování zlepšování KB.
- Podílení se na řízení kontinuity činností (zejména stanovení priorit obnovy služeb).

§ 6 Bezpečnost lidských zdrojů

- Stanovení pravidel rozvoje bezpečnostního povědomí. Vstupní i pravidelná školení lze zajistit zdarma v e-learningu od NÚKIB na osveta.nukib.gov.cz.
- Kontrola dodržování nastavených pravidel a stanovení postupů pro případy jejich porušení.

§ 7 Řízení kontinuity činností

- Stanovení priority, pořadí a postupů obnovy.
- Vytváření pravidelných záloh informací, dat a konfigurací nezbytných pro případ obnovy.

§ 11 Řešení kybernetických bezpečnostních incidentů

- Stanovení, jakým způsobem mají zaměstnanci hlásit neobvyklé chování technických aktiv.
- Příprava procesů pro řešení případných incidentů (posouzení, vyhodnocení, řešení) před samotným hlášením NÚKIB.

4.5 Vyhodnotitelná bezpečnostní opatření

U níže uvedených opatření musí povinná osoba sama vyhodnotit, zdali a v jaké míře je bude zavádět, aby to bylo přiměřené jejím bezpečnostním potřebám. Je také možné a v praxi vhodné zavádění rozplánovat v čase v dokumentu „**Přehled bezpečnostních opatření**“.

§ 8 Řízení přístupu

- Zavedení principů nejnižších oprávnění, jedinečných identifikátorů a oddělování privilegovaných účtů.
- Řízení přístupových práv v celém životním cyklu (přidělování, změna, odebírání, přezkum).
- Řízení mobilních zařízení a zařízení mimo správu organizace.
- Řešení fyzické bezpečnosti k ochraně aktiv před fyzickým poškozením, krádeží apod.

§ 9 Řízení identit a jejich oprávnění

- Vícefaktorová autentizace pokud je možné ji nasadit, pokud to možné není, tak odolné kryptografické klíče/certifikáty, pokud ani to není možné, tak autentizace uživatelským jménem a heslem při splnění požadavků heslové politiky.
- Změna výchozích, jednorázových a kompromitovaných hesel. Zajištění důvěrnosti autentizačních údajů.
- Zabezpečení administrátorských účtů určených zejména pro případ obnovy.

§ 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí

- Ochrana perimetru komunikační sítě, např. pomocí firewallu pro ochranu a blokování nežádoucí komunikace.
- Ochrana před malware na koncových stanicích a serverech, např. formou antiviru či EDR.

§ 12 Bezpečnost komunikačních sítí

- Rozdělení vnitřní komunikační sítě do menších systematických celků a řízení komunikace mezi nimi za účelem zvýšení jejich bezpečnosti.
- Omezení komunikace na vnějším síťovém perimetru například pomocí firewallu.
- Užívání aktuálně odolných a bezpečných síťových protokolů.
- Řízení vzdáleného připojování a vzdálené správy.

§ 13 Aplikační bezpečnost

- Aplikování bezpečnostních aktualizací.
- Evidence a ochrana nepodporovaných technických aktiv, pro které nevycházejí aktualizace.

- Pravidelné skenování zranitelností relevantních technických aktiv a ošetření zjištěných nedostatků.

§ 14 Kryptografické algoritmy

- Užívání aktuálních kryptografických algoritmů a zohledňování doporučení NÚKIBu v této oblasti.
- Zajištění bezpečné hlasové, audiovizuální, textové (zejména e-mailové) a nouzové komunikace.

5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
6. prosince 2024	1.0	OREG/OK	Vytvoření dokumentu