Klíčová aktivita KA06

Kyberbezpečnost

Manažerské shrnutí

Dokument byl zpracován v rámci realizace projektu

„Efektivní řízení rozvoje obcí jako základní předpoklad efektivnosti výkonu veřejné správy

a poskytování veřejných služeb z úrovně obcí“,

registrační číslo projektu: č.CZ.03.4.74/0.0/0.0/15\_019/0010159

Obsah

[Úvod 3](#_Toc122434133)

[Východiska 3](#_Toc122434134)

[Shrnutí 4](#_Toc122434135)

[Postupy 4](#_Toc122434136)

[Dokumentace 5](#_Toc122434137)

[Osvětové: 5](#_Toc122434138)

[Strategické: 5](#_Toc122434139)

[Procesní: 6](#_Toc122434140)

[Pomocné: 6](#_Toc122434141)

[Shrnující a doporučující: 6](#_Toc122434142)

[Stručné shrnutí situace v jednotlivých obcích 6](#_Toc122434143)

[Obec I. Typu 6](#_Toc122434144)

[Obec II. Typu 7](#_Toc122434145)

[Obec III. Typu 7](#_Toc122434146)

[Městská část 8](#_Toc122434147)

[Město 8](#_Toc122434148)

[Metodická doporučení 9](#_Toc122434149)

[Závěr 11](#_Toc122434150)

# Úvod

Cílem této klíčové aktivity je vytvoření specializovaného rámce v oblasti kyberbezpečnosti pro vybrané subjekty, včetně provedení a individuálního školení pro tyto vybrané subjekty. Rámec obsahuje vzorové dokumenty a pomůcky. Aktivita je zaměřena na vytvoření metodik, resp. doporučených kroků, které by měly obce provést pro zajištění odpovídající úrovně kybernetické a informační bezpečnosti obcí.

Základním momentem celé problematiky kybernetické a informační bezpečnosti informační (KIB) a komunikační infrastruktury obce je to, že za ni zodpovídá statutár. Tento fakt nezávisí na tom, zda obce spadají nebo ne pod zákon 181/2014 Sb. o kybernetické bezpečnosti (ZoKB). Je nutno si uvědomit, že KIB není otázkou zákonů, ale že je otázkou pudu sebezáchovy obce a tím i jejího vedení. V případě úspěšného hackerského útoku zde existuje řada rizik, a to od reputačního, přes rizika finančních ztrát, riziko úniku osobních údajů a mnoho dalších.

# Východiska

V tomto okamžiku schválená evropská směrnice pro bezpečnost sítí a informací, známá pod zkratkou NIS2, dost výrazně mění a tím pádem i zpřísňuje pohled na zajištění kybernetické a informační bezpečnosti obecně. Rozšiřuje záběr regulace na mnohonásobně větší počet subjektů, které dosud pod regulaci kybernetické a informační bezpečnosti nespadaly, a to ze současných cca 360 na budoucích minimálně 6 tisíc subjektů. Zkušenosti ze Slovenské republiky už ale říkají, že jich bude spíše 10 – 15 tisíc. Což zcela určitě vyvolá obrovský přetlak poptávky nad nabídkou odborníků na KIB na trhu práce. Změny v evropské legislativě (NIS2) se musí cestou harmonizace promítnout i do národní legislativy, tedy si vynutí změny v ZoKB. Předpokládanou, respektive jistou změnou bude i to, že pod ZoKB „spadnou“ i obce. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) připravuje novelu ZoKB v tom smyslu, že všechny obce s rozšířenou působností (ORP) se stanou osobami povinnými vůči ZoKB a budou muset zavést organizační a technická opatření, tak jak jsou definována v ZoKB a upřesněna v navazujících předpisech, zejména pak ve vyhlášce 82/2018 Sb. (Vyhláška o kybernetické bezpečnosti – VoKB). Zatím není úplně jasno, jak bude vypadat definitivní znění novely ZoKB (v lednu202š má být k dispozici pro diskusi v odborné veřejnosti), nicméně to vůbec nebrání tomu, aby se obce otázkami KIB intenzivně zabývaly už teď. Faktem ovšem je, že stav, kdy obce dosud nespadají pod ZoKB způsobil to, že obce nebyly a nejsou připraveny na nebezpečí, která masivní digitalizace agend a propojení všech se všemi přináší. A proto není důvod čekat na legislativní úpravu.

# Shrnutí

V rámci klíčové aktivity byly osloveny některé obce všech typů, zda by se nechtěly do této klíčové aktivity zapojit. Cílem bylo získat cestou osobních návštěv a konzultací přehled o situaci v oblasti KIB u subjektů Obec I. Typu, Obec II. Typu, Obec III. Typu, Městská část/obvod, Statutární město. Díky osobním kontaktů došlo poměrně hladce k dohodě s obcí Košíky na Zlínsku) – obec I.typu, dále s obcí Planá (u Mariánských lázní) – obec II.typu, s městem Židlochovice – obec III.typu, s městskou částí Praha 5 – Městská část/obvod a s městem Chomutov – statutární město. Nejedná se sice o statisticky významný vzorek, ale tento průzkum jen potvrdil dlouholetou zkušenost odborníků na kybernetickou a informační bezpečnost, že jelikož obce nespadají pod zákon o kybernetické bezpečnosti 181/2014 Sb. tak oblast KIB nevnímají jako významnou. Obecně lze říct, že zajištění KIB závisí na osvícenosti pracovníků, zodpovídajících za provoz informačních a komunikačních technologií (ICT). A z jejich strany je přístup ke KIB dán spíše snahou o zajištění bezproblémového provozu ICT. Z toho plyne, že zajištění KIB je zúženo na čistě technická opatření jako zajištění ochrany proti škodlivému kódu (antiviry), ochrana síťové infrastruktury (firewally) apod. Organizační opatření jsou vnímána jako obtěžující a vedení dokumentace jako něco, co se udělá až potom (což nikdy nenastane).

Je ovšem nutno říct, že jsem se při návštěvách a konzultacích nesetkal s neochotou tento stav napravit. Z konzultací vyplynula nutnost vytvořit takovou metodiku, která by byla ve svém rozsahu odpovídající velikosti obce (ne vždy se shoduje s typem obce) a složitosti její informační infrastruktury. Těžko lze chtít po vedení obce, ve které používají dva počítače, aby zavedlo bezpečnostní politiky KIB v plném rozsahu (cca 70 stran jen politik).

U obcích I. a II. typu byl zvolen přístup minimální administrativní náročnosti. Je zřejmé, že tam, kde se o počítače stará externí odborník (a když je dobře, tak pod smlouvou), tak jde spíše o vytvoření stručného dokumentu, kde budou základní informace o tom kde, co je a kde to nalézt, kdyby se „něco“ stalo.

Pro obce III. Typu a výše (ORP) s ohledem na jejich budoucí roli osoby povinné vůči ZoKB, byly vytvořeny vzorové dokumenty, které jsou určeny k vytvoření vnitřního legislativního rámce v obci tak, aby bylo možné se o tuto vnitřní legislativu opřít při přijímání organizačních a technických opatření a také obhájit nároky na finanční, lidské i časové kapacity.

## Postupy

Všechny výše uvedené obce byly navštíveny min. dvakrát a byly provedeny jekési analýzy stavu, ze kterých vzešla doporučení, resp. byly zpracovány dokumenty pro zlepšení stavu. Detailněji je toto popsáno v následujících kapitolách.

## Dokumentace

Na základě získaných zkušeností byla vytvořena sada dokumentů těchto zaměření:

### Osvětové:

Dokument Úvod do problematiky a metodický rámec kybernetické bezpečnosti – **Příloha\_1\_Úvod do problematiky a metodický rámec\_Kybernetická a informační bezpečnost.** Tento dokument je určen k srozumitelnému vysvětlení problematiky KIB včetně vysvětlení souvislostí v širším kontextu. Je v něm uvedena řada negativních důsledků nesprávného chápání KIB včetně příkladů z reálné praxe. Jsou zde uvedeny i základní otázky, na které by si měla každá obec najít odpovědi a také základní zásady KIB, které by každý uživatel informačních a komunikačních technologií (ICT) měl znát. Dokument je určen k popularizaci problematiky KIB a měl by být přijatelnou formou dostupný všem uživatelům ICT – např. Intranet. Ambicí tohoto dokumentu není citovat paragrafy legislativy i když její základní principy vysvětluje. Jeho úlohou je popularizovat u uživatelů otázky KIB a srozumitelnou formou jim vysvětlit, jaké zásady KIB mají v základní úrovni dodržovat a na jaké otázky by si vedení obce mělo umět nalézt odpovědi.

### Strategické:

 Byly vytvořeny dva vzory základních strategických dokumentů:

Politika bezpečnosti informací – **Příloha\_2\_Politika\_bezpečnosti\_informací**

Tento dokument je deklarací vedení obce, že chápe důležitost KIB a že přijímá zodpovědnost za její řešení. Je to dokument, kterým by vedení obce, která už má složitější informační infrastrukturu a spravuje sadu informačních aktiv s vyšší hodnotou, mělo deklarovat svoji vůli kybernetickou bezpečnost řešit.

Politika organizačních a technických opatření kybernetické bezpečnosti – **Příloha\_3\_Politika organizačních a technických opatření kybernetické bezpečnosti\_vzor**

Tento dokument obsahuje všechny vzorové politiky, které v současné době vyžaduje VoKB. Jsou do té míry zobecněny, že je lze použít v jakékoliv obci. Smysl to ovšem dává v obcích od III. typu výše a v některých větších obcích II. typu. Implementace těchto politik musí být řízená se stanovením priorit. Průzkum ukázal, že hlavně technická opatření podle těchto politik zavedena jsou, chybí ale jejich formální zavedení a už výše zmíněná dokumentace. Průzkum také ukázal, že celá řada opatření je zavedena a i dokumentována, ale jinak se jmenují. Nebylo cílem této aktivity silou překlápět zažité procesy. Na příkladu statutárního města Chomutova lze ilustrovat to, že opravdu jsou opatření zavedena, ve značné míře i dokumentována v provozní dokumentaci ICT, ale se jinak jmenují. Hlavním cílem bylo tedy nalezení pochopení a tím i vnímání důležitosti přijetí opatření. Zmíněný dokument (příloha č.3) je tedy jakousi knihovnou politik, které lze postupně implementovat do prostředí obce. Dokument je strukturován tak, že v úvodu kromě obvyklých kapitol, jako jsou pojmy, zkratky, zodpovědnosti atd. obsahuje u stručné popisy jednotlivých politi s tím, komu jsou primárně určeny.

### Procesní:

Byl vytvořen dokument Záznam o bezpečnostním školení zaměstnance v oblasti bezpečnosti informací – soubor **Příloha\_4\_Záznam o proškolení\_Kybernetická a informační bezpečnost**.Tento dokument je velmi důležitý, neboť je záznamem o prokazatelném proškolení zaměstnance o zásadách kybernetické a informační bezpečnosti. Měl by být aplikován v okamžiku, kdy nový zaměstnanec nastoupí do práce, a to prokazatelně. Stejně jako je to u BOZP. Tento dokument lze použít i jako periodickou nebo ad-hoc připomínku základních zásad KIB. Při e-mailové edukační kampani apod.

### Pomocné:

Dokumenty v této skupině jsou pomůckami, které umožňují obcím zmapování informační infrastruktury obce a tím i nalezení slabých míst. Jedná se o tabulky, které si jednotlivé obce buď samy nebo ve spolupráci s dodavateli vyplnily hlavně pro vlastní potřebu. Do jisté míry se jedná o jakousi sebereflexi, jak na tom vlastně obec s KIB je. Práce s těmito dokumenty je čistě na vůli vedení obce. V každém případě se jedná o dokument, jehož vypovídací hodnota závisí na ochotě těch, kteří jej vyplňují, říct si pravdu.

Jsou to tyto dokumenty:

Posouzení KIB – soubor **Příloha\_5\_Posouzeni KIB**. V tomto dokumentu se jedná o sebehodnocení obce jak na tom v základních bodech kybernetické a informační bezpečnosti je. Jedná se o jakýsi maturity model. Je v zásadě úplně jedno, kdy je tento dokument vyplněn. Je podstatné, aby byl pravdivý a živý, protože situace v KIB se neustále mění.

Služby a aplikace \_ soubor **Služby\_aplikace** - Příloha č.6. Tento dokument, naplněný pravdivými informacemi, je velmi důležitý v případě kybernetického incidentu. Pečlivě vyplněný může u obcí I. a II. typu sloužit i jako plán zajištění kontinuity činností. Což znamená podklad pro řízené zvládnutí kybernetických bezpečnostních incidentů.

Katalog aktiv s kontakty – soubor **Příloha\_7\_Katalog aktiv s kontakty.** Tento dokument je zjednodušenou verzí dokument Služby a aplikace. Aplikovatelný v malých obcích s jednoduchou infrastrukturou

Aktiva, maturity model, garanti – **soubor Přílloha\_9\_Aktiva\_maturity model\_garanti.** Poměrně sofistikovaná varianta dokumentu Služby a aplikace. Vychází z vyhlášky 82/2018 Sb. Umožňuje vytvoření maturity modelu ve vztahu k této vyhlášce. Umožňuje základní evidenci aktiv s jejich hodnocením z pohledu Důvěrnosti, Integrity a Dostupnosti, umožňuje také základní evidenci garantů aktiv ve smyslu této vyhlášky

### Shrnující a doporučující:

Každá obec obdržela dokument Manažerské shrnutí a doporučená opatření. V tomto dokumentu byla shrnuta zjištění z konzultací i s doporučeními, jak postupovat dále v oblasti KIB. Zároveň tento dokument obsahuje stručnou SWOT analýzu. Z pochopitelných důvodů stejně jako dokumenty v předchozí kapitole po vyplnění nemohou být veřejné. Obce jejich poctivým vyplněním odhalují nejen své silné stránky, ale hlavně slabiny v oblasti KIB, což může být velmi nebezpečné.

#

# Stručné shrnutí situace v jednotlivých obcích

## Obec I. Typu

Obec

Byly zde provedeny 2 návštěvy.

První návštěva se týkala sběru informací, vysvětlení účelu klíčové aktivity a vysvětlení základů kybernetické a informační bezpečnosti. Jednání se zúčastnil pan starosta a koordinátorka komunitního centra, která je zároveň jakýmsi superuserem ICT. Bylo konstatováno, že informační a komunikační infrastruktura je velmi jednoduchá. Skládá se z jednotek počítačů, které nejsou propojeny do počítačové sítě. Překvapivě kvalitní je konektivita do Internetu, která je realizována optickým kabelem. Administraci provádí externí firma.

Druhá návštěva se týkala hlavně vysvětlení práce s dokumentem **Katalog aktiv s kontakty** – příloha č.7, což je zjednodušená tabulka, vycházející z dokumentu **Služby\_aplikace.** Dále bylo provedeno proškolení obsahu dokumentu „Záznam o bezpečnostním školení zaměstnance v oblasti bezpečnosti informací“ i to, jak s ním dále pracovat, tzn.

Doporučení jsou shrnuta v dokumentu Manažerské shrnutí, který byl předán panu starostovi

## Obec II. Typu

Město

Byly zde provedeny 2 návštěvy a jedna videokonference.

První návštěva měla informační charakter a kromě zástupců SMO se ji zúčastnila tajemnice městského úřadu a zaměstnanec, který je neoficiálně pověřen správou IT. Informační infrastruktura městského úřadu je jednoduchá. Administraci provádí externí firma, která zajišťuje i kybernetickou bezpečnost z hlediska technologií.

Druhá návštěva se týkala vysvětlení práce s dokumenty a to zejména **Politika bezpečnosti informací, Služby\_aplikace, Záznam o proškolení\_Kybernetická a informační bezpečnost.**

Třetí schůzka proběhla cestou videokonference a primárně v ní šlo o vyjasnění technických aspektů informační infrastruktury s dodavatelem IT služeb. Ten byl upozorněn na zjištěné nedostatky. Opět zde byl probrán dokument **Služby\_aplikace**. Bez dodavatele s tímto dokumentem nelze pracovat a už vůbec jej nelze udržovat v aktuálním stavu.

Doporučení jsou uvedena v dokumentu Manažerské shrnutí, který byl předán paní tajemnici. Toto manažerské shrnutí obsahuje i stručnou SWOT analýzu

## Obec III. Typu

Město

Byly zde provedeny tři návštěvy.

První návštěva měla informační charakter. Zúčastnila se jí paní tajemnice a v podstatě šlo jen o vysvětlení klíčové aktivity a domluvení další spoluprác.

Druhá schůzka proběhla v oddělení IT a šlo o pochopení informační infrastruktury.

Třetí schůzka se týkala v prví části organizačních opatření v KIB. Byly vysvětleny obě politiky **Politika bezpečnosti informací** a **Politika organizačních a technických opatření kybernetické bezpečnosti** a dokument **Záznam o proškolení\_Kybernetická a informační bezpečnost.** V technické části schůzky byla vysvětlena práce s dokumenty **Posouzení KIB** a **Služby a aplikace.** Pracovníci IT oddělení tyto dokumenty zpracovali velmi pečlivě. Dále proběhla prezentace technických opatření podle vyhlášky 82/2018 Sb.

Doporučení jsou uvedena v dokumentu Manažerské shrnutí, který byl předán paní tajemnici. Toto manažerské shrnutí obsahuje i stručnou SWOT analýzu.

## Městská část

Městská část

Městská část je ve vztahu k ostatním zde uvedeným obcím ve zvláštním postavení, a to ze dvou základních důvodů. Prvním důvodem je to, že už na jaře loňského roku byla na úřadu městské části zřízena funkce manažera kybernetické bezpečnosti, takže organizačně je kybernetická a informační bezpečnost pokryta. Co se týká technické stránky KIB, ta je zajištěna dodavatelsky. Druhým důvodem je to, že na jaře roku 2022 byl ÚMČ pod kybernetickým útokem a všechny systémy byly z bezpečnostních důvodů vypnuty na 9 dnů. Vzhledem k tomu, že ÚMČ disponoval plánem pro obnovu systémů (Disaster Recovery Plan - DRP) a měl k dispozici kvalitní zálohy, tak nedošlo k výraznějším ztrátám informací. ÚMČ přijal **Politiku informační bezpečnost**i a tím si vytvořil legislativní rámec pro postupné zavádění opatření KIB. Vzdělávání zaměstnanců v oblasti KIB je zavedeno a je využíváno e-learningu NÚKIB. V podstatě chyběl další krok a sice přijetí a implementace dokumentů **Politika organizačních a technických opatření kybernetické bezpečnosti** a **Záznam o proškolení\_Kybernetická a informační bezpečnost.** Implementace dokumentu **Posouzení KIB**, zatím nedává smysl, protože ÚMČ je ve fázi budování nové informační infrastruktury (tzv. Zelená louka). Dokument **Služby a aplikace** je nahrazen již existujícím DRP. Metodické vedení zavádění KIB řídí manažer kybernetické bezpečnosti. Dokumentace je součástí projektu Zelená louka.

## Město

Statutární město

Zde proběhly dvě návštěvy. První byla informační s tím, že byla vysvětlena důležitost zavedení KIB.

Druhá byla zaměřena primárně na dokument **Politika organizačních a technických opatření kybernetické bezpečnosti** (politika)a na jeho jednotlivé body. Po technické stránce je KIB informační infrastruktury zajištěna velmi kvalitně, a to i přes její poměrně komplikovanou a rozsáhlou (v porovnání s ostatními obcemi) strukturu. Jako všude jinde i zde je problém s dokumentací. Nicméně bylo zjištěno, že celá řada požadavků politiky už je zahrnuta ve směrnici, kterou je definován provoz IT. Vedoucí oddělení IT přislíbil zpracovat „propojení“ paragrafů politiky s touto směrnicí.

# Metodická doporučení

Každá obec bez ohledu na typ, by se primárně měla zaměřit na zajištění kontinuity činností. Je nutno znát odpovědi na otázky uvedené v dokumentu **Kybernetická a informační bezpečnost Úvod do problematiky a metodický rámec**

* Chceme vůbec kybernetickou a informační bezpečnost řešit?
* Víme, kde co máme? (katalog informačních aktiv – služeb, serverů, systémů, aplikací atd.) Zde lze s výhodou použít dokument
* Víme, co s čím komunikuje? (identifikované datové toky)
* Víme, jak jsme na tom se zabezpečením? (sebehodnocení – jaká opatření máme zavedena, jak jsou účinná)
* Známe rizika? (víme co hrozí, když se něco stane – co nebude fungovat, jaké služby nebudeme schopni poskytovat, jaké sankce za to hrozí, co na to řeknou občané atd.)
* Víme, kdo co spravuje? (Máme přehled o správcích našich technologií a systémů, a to i externích, kdo má od čeho klíče a to i ty fyzické)
* Máme kontaktní matici? (Víme, komu zavolat, když se něco stane)
* Víme jak z průšvihu? (Máme plán, jak průšvih zvládnout)
* Víme, kde máme, a jak máme použít zálohy?
* Víme, v jakém pořadí máme spouště po výpadku informační systémy (aplikace)?
* Víme, kdy a s jakým výsledkem jsme si obraz o stavu kontrolovali – testovali?
* Víme, jak jsme na zjištění reagovali? (Přijali jsme nápravná opatření)
* Máme všechno dokumentováno? (A vytištěno?)
* Jsou naši uživatelé dostatečně obezřetní? (Prokazatelně a pravidelně proškolení)
* Co děláme pro to, aby byli? (máme na to plán?)
* Máme pod kontrolou dodavatele? (řekli jsme jim, že po nich chceme bezpečné chování)

Pro zajištění kontinuity činností je naprosto zásadní, aby vedení obce odpovědi na tyto otázky znalo

**Pro obce I. a II. typu tedy platí**

Využít přílohy **č. 7 Katalog aktiv s kontakty** nebo (podle velikosti informační infrastruktury) **č.6 Služby a aplikace** a **č.5: Posouzení KIB** (s tím, že některé body se obce netýkají, ale i to je dobré vědět)

Tím jsou vytvořeny základní podklady pro úspěšné zvládnutí případného výpadku služeb, ať už je způsoben čímkoliv.

S těmito vyplněnými dokumenty je nutno pracovat následujícím způsobem:

* Udržovat je (např. ve spolupráci s dodavatelem IT služeb) v aktuálním stavu a vědět kde jsou
* Mít je k dispozici i v tištěné podobě
* Pravidelně (jednou ročně) hodnotit jejich účinnost (např. jestli bezpečnostní technologie odpovídají současným trendům v oblasti kybernetických hrozeb)
* Na základě těchto dokumentů mít zpracovaný plán obnovy. Ten musí obsahovat:
	+ Kontaktní matici tzn. koho budete kontaktovat:
		- Pro technickou pomoc s obnovou (typicky dodavatel IT služeb, specialisté pro řešení výpadků apod.)
		- Pro provozní pomoc (typicky správci infrastruktury)
		- Pro organizační zajištění (kdo zajistí vstup do prostor, kdo popíše incident, kdo píše zápis o průběhu řešení incidentu, uvaří kávu atd.)
		- Pro informovanost (typicky vedení obce, nadřízený orgán, dotčené subjekty)
		- Pro nahlášení možného trestného činu (PČR)
		- Pro nahlášení kybernetického incidentu (NÚKIB, Úřad pro ochranu osobních údajů)

Na základě zpracovaných výše uvedených dokumentů stanovit pořadí spouštění aplikací, resp. informačních systémů. Při stanovení priorit brát v úvahu ohrožení plnění zákonných povinností např. nesplněním lhůt. Dále ohrožení poskytování klíčových služeb občanům. Plnění smluvních závazků atd. Při stanovování priorit obnovy je důležité vědět, co se dá zařídit „jinak“. Například je zbytečné stresovat a zdržovat odborníky, kteří odstraňují následky havárie, žádostmi o urychlenou obnovu chodu aplikace pro evidenci psů. To se dá řešit spuštěním technologie „tužka a papír“.

Důležité je informovat všechny zaměstnance o tom co v době do dořešení výpadku nesmí dělat. Například snaha o spuštění zasažené stanice může vést ke zhoršení situace a ztížení snahy o obnovu chodu informační infrastruktury.

Je velmi důležité mít připravenou komunikační strategii, jak výpadek služeb bude komunikován s občany. Například umístěním informací na stránkách obce, obecním rozhlasem, zajištěním náhradní komunikace s klíčovým pracovníky úřadu. Občany je nutno informovat o tom, které služby jsou omezeny, které jsou vypnuty úplně, které jsou zajištěny náhradním řešením a které fungují bez omezení

Znovuspuštění informační infrastruktury a obnovu ze záloh proveďte tehdy, až budete mít maximální možnou jistotu, že je vaše infrastruktura „čistá“ a že jsou „čisté“ i vaše zálohy, aby nedošlo k opětovnému zavlečení nákazy.

Aby se minimalizovala pravděpodobnost, že k výše uvedené situaci dojde, je nutno mít obezřetné uživatele, ať už je jejich vztah k úřadu jakýkoliv. Zaměstnanci, externí pracovníci, brigádníci i dodavatelé musí dodržovat zásady KIB. Pro nové i současné uživatele je nutno zajistit prokazatelně základní proškolení s využitím **přílohy č. 4 Záznam o bezpečnostním školení zaměstnance v oblasti bezpečnosti informací.** Pro rozšíření těchto znalostí využijte e-learningu NÚKIB <https://osveta.nukib.cz/dk-22-24>.

**Pro obce III. typu a výše** platí to stejné s tím, že s ohledem na vysoce pravděpodobný dopad legislativy kybernetické bezpečnosti na tyto obce, budou mít mnohem více povinností. Tyto povinnosti jsou stručně vysvětleny v kapitole **E.** **přílohy č. 1 Kybernetická a informační bezpečnost Úvod do problematiky a metodický rámec.** Jedná se sadu organizačních a technických opatření, která v přiměřené míře bude muset každá obec přijmout.

Jako první krok doporučuji projednat s vedením dokument **Příloha č.2: Politika bezpečnosti informací**, kterým vedení obce deklaruje to, že se kybernetickou a informační bezpečností bude zabývat a že na přijetí odpovídajících opatření uvolní finanční, lidské a časové zdroje. Pro inspiraci přikládám i důvodovou zprávu pro jednání Rady, **Příloha č.8 Důvodová zpráva Politika kybernetické a informační bezpečnosti.** Současně je nutno pracovat s výše uvedenými dokumenty, tak jako v případě obcí I. a II. typu s tím, že rozsah bude pravděpodobně větší. Je na zvážení, zda nebude pro vás výhodnější místo dokumentu **Příloha č.6: Služby aplikace** použít dokument **Příloha č.9 Aktiva, maturity model, garanti**, který je sofistikovanější a vyžaduje už určitou zkušenost. Paralelně lze pracovat na vydání dokumentu viz **Příloha č.3: Politika organizačních a technických opatření kybernetické bezpečnosti.**  Který obsahuje kompletní sadu politik, vyžadovaných vyhláškou o kybernetické bezpečnosti. Tento dokument je v gesci tajemnice/tajemníka úřadu a definuje interní legislativní rámec pro zavedení opatření KIB. Je připraven na to, aby byl okamžitě použitelný v každé obci, stačí zaměnit XXXXXX za název obce-úřadu. Dokument je úmyslně maximálně obecný, aby jej nebylo nutno často aktualizovat. Na tento dokument proto potom musí navazovat provozní směrnice, které řeší detaily. Je dobré si udělat analýzu už existující dokumentace, jestli už nejsou některá témata řešena, jen „se to jmenuje jinak“.

# Závěr

Situace pro obce I. a II. typu je poměrně jasná v tom, že teď už lze KIB do těchto obcí zavést s pomocí tohoto dokumentu. U obcí vyššího typu je zatím nejasno z důvodu prací na harmonizaci národní legislativy se směrnicí NIS2, které se promítnou do podoby zákona o kybernetické bezpečnosti a navazujících předpisů. Otázkou je, jak ve vztahu k obcím tento zákon bude přísný. Nicméně přijmout opatření KIB v obcích je životní nutností a pokud se obce budou řídit výše uvedenými doporučeními, tak zcela určitě nic nepokazí.

**Seznam příloh:**

Příloha č.1: Kybernetická a informační bezpečnost Úvod do problematiky a metodický rámec

Příloha č.2: Politika bezpečnosti informací

Příloha č.3: Politika organizačních a technických opatření kybernetické bezpečnosti

Příloha č.4: Záznam o bezpečnostním školení zaměstnance v oblasti bezpečnosti informací

Příloha č.5: Posouzení KIB

Příloha č.6: Služby aplikace

Příloha č.7: Katalog aktiv s kontakty

Příloha č.8 Důvodová zpráva Politika kybernetické a informační bezpečnosti

Příloha č.9 Aktiva, maturity model, garanti