Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Informační
a komunikační
technologie

Strategický dokument pro oblast: Informační a komunikační technologie a (kybernetická) bezpečnost

Svaz měst a obcí České republiky

Projekt: Realizace SMART ČESKO v praxi obcí a měst
Reg. č.: ***CZ.03.4.74/0.0/0.0/15_025/0016927***

SMO
SVAZ MĚST A OBCÍ ČESKÉ REPUBLIKY

SMART Česko

Obsah

SMART strategický dokument – Informační a komunikační technologie a (kybernetická) bezpečnost

Vize

Cílem postupné digitalizace činností a rozvojem bezpečných informačních a chytrých (SMART) technologií je zajistit poskytování kvalitních služeb občanům, zjednodušit jim komunikaci s úřadem, aby co nejvíce věcí mohli řešit například skrze mobilní technologie z pohodlí jejich domova a přitom zaručit, že nedojde k narušení jejich bezpečí v kybernetickém prostoru.

Vymezení řešené oblasti

Kvalita života občanů v obcích se ve značné míře odráží od toho, jak obec funguje, jak s občany komunikuje, jaké služby poskytuje a jak na podněty a návrhy občanů reaguje. Kvalitnímu poskytování služeb občanům ve značné míře napomáhají SMART digitální technologie, které si díky komunikační infrastruktuře v obcích rychle najdou cestu k občanům. Již dnes je možné na Portálu občana, provozovaném Ministerstvem vnitra, nalézt řadu dlaždic s elektronickými službami obcí. Tento trend se postupně dotkne všech obcí, protože požadavky občanů na řešení záležitostí s obcí a veřejnou správou vůbec rostou, mimo jiné i v souvislosti s přijetím Zákona o právu na digitální služby. Značně tomu napomohlo od ledna 2021 využívání bankovní identity, pro ověřování při poskytování služeb veřejné správy. Pro bezpečnost těchto činností je nezbytné, aby byly zajištěny proti zneužití kybernetickými útočníky, což si musí uvědomit každý poskytovatel těchto služeb, potažmo každá obec.

Dynamický rozvoj informačních a komunikačních technologií se dnes dotýká naprosto všech oblastí lidského života. Doprava, zdravotnictví, obchod, energetika, služby a řada dalších oblastí se dnes bez ICT neobejdou. Nároky na jejich využívání postupně rostou a názorně je to vidět na nastupující mladé generaci, která na využívání komunikačních a digitálních nástrojů klade stále větší důraz a stává se tak de-facto článkem společnosti, který udává často směr a impulzy dynamickému rozvoji. A protože i správa věcí veřejných je neoddělitelnou součástí fungování lidské společnosti, tak je nezbytné, aby se i veřejná správa kontinuálně modernizovala a rozvíjela a využívala SMART digitální technologie.

Cílem těchto kroků musí být snaha zkvalitnit, zrychlit a přiblížit výkon veřejné správy blíže občanovi, aby si mohl své záležitosti řešit z pohodlí svého domova a v obci, kde bydlí. Tak jako dnes občané běžně využívají bankovní elektronické služby, tak stejným způsobem musí mít občan možnost využívat i služby veřejné správy, a to nejen na úrovni státu, jako jsou například služby Czech POINT (výpis z Registru trestů, informace z Katastru nemovitostí a řada dalších), ale měl by mít možnost elektronickou cestou vyžívat i služby poskytované přímo jeho obcí. Elektronicky řešit poplatkové povinnosti, být informován o aktuálním dění, spolupodílet se na rozhodování například formu anket či vznášení podnětů, být včas informován o omezeních či nebezpečích.

Proto, aby obec mohla takovéto a v budoucnu i další služby poskytovat je nezbytné si zajistit kvalitní komunikační infrastrukturu, pro dostatečné a bezpečné spojení jak se službami státu, tak i s občany. Určitě je vhodné se zamyslet nad vybudování

komunikační sítě, která je již dnes vnímána řadou obcí jako nebytná součást fungování obce.

Současně je při rozvoji digitálních technologií nezbytné myslet na nebezpečí kybernetických útoků. Je totiž úplně jedno, zdali obce pro své fungování a výkon veřejné správy využívá jeden počítač, či jich provozuje 50 či ještě více. Je proto potřeba již dnes kybernetickou bezpečnost nepodceňovat a do budoucna s ní počítat.

Popis současného stavu

Zajišťování výkonu veřejné správy je v dnešní době významně kvalitativně závislé na úrovni využívaných informačních a komunikačních technologií což stále více závisí i na jejich bezpečnosti. Kvůli dynamičtějšímu způsobu života, složitosti legislativy, snahám přiblížit výkon veřejné správy co nejblíže k občanovi a zajistit mu co největší komfort, by orgány veřejné moci bez informačních technologií vůbec nemohly fungovat. Kromě interních systémů zajišťující provoz konkrétních agend a činností (stavební úřad, správa daní a poplatků, řešení přestupků a pokut, výdej oprávnění k parkování, sociálně právní ochrana dětí, svoz a likvidace komunálního odpadu a řada dalších), je na obcích řešena řada činností, které na obec přenesl stát (tzv. výkon přenesené působnosti státu). Tam jsou obce de facto prodlouženou rukou státu (výdej občanských průkazů, cestovních dokladů, řidičských oprávnění a dalších). Mimo tyto činnosti si řada obcí buduje vlastní „SMART“ řešení ve formě elektronické nabídek služeb (tzv. portálová řešení), postavená na internetových technologiích, jejichž prostřednictvím dokáže své služby nabízet občanům i v pohodlí jejich domova. Jedná se především o různá portálová řešení, jejichž dlaždici (odkaz) je možno nalézt na Portálu občana Ministerstvem vnitra. Jeho prostřednictvím může občan provést různá podání a činnosti (přihlásit se k poplatku za svoz odpadu, přihlásit psa, požádat o parkovací kartu), dále pak systémy pro rezervaci času úředníků, pro řešení jeho záležitostí a samostatnou oblastí je poskytování služeb Czech POINT, opět provozovaným Ministerstvem vnitra, kde občan může získat řadu výpisů a dokumentů. V poslední době se začínají na obcích objevovat nová řešení, která řeší sběr a prezentaci dat z různých SMART technologií. Jedná se především o data ze senzorů a čidel, monitorující odběr energií, kvalitu ovzduší, hustotu dopravy, zaplnění odpadových nádob, obsazenost parkovacích ploch, polohu vozidel MHD či polohu a pohyb sdílených dopravních prostředků a řadu dalších. Vedle portálů neboli prezentačních dashboardů (veřejných či operátorských), se dnes obce silně orientují na nástroje energetického managementu, které umožňují sofistikovaně sbírat data o spotřebě energií a různých komodit, upozorňují na nestandardní stavy, dokáží predikovat možné úspory a některé z nich zahrnují i nástroje facility managementu, týkající se revizí a certifikací vybavení budov.

Vedle těchto snah a činností, tj. poskytovat SMART nástroje pro občany, si obce uvědomují, že budoucnost kvalitního fungování veřejné správy je do značné míry závislá na dobré komunikační infrastruktuře. Z těchto důvodů již dnes řada obcí připravuje či realizuje budování obecní komunikační sítě, nebo řeší její dlouhodobý pronájem s komerčními poskytovateli. V řadě případů se například pro uložení optických tras využívají výkopové práce liniových staveb, ke kterým se tyto komunikační trasy či jejich ochranné prvky přikládají. Pro financování je často využíváno dotačních titulů z Evropské unie.

I přes veškeré dobré úmysly poskytovat kvalitní služby občanům v pohodlí jejich domova a zajistit jim bezproblémovou vysokokapacitní komunikaci, obce nesmí zapomínat na zajištění kybernetické bezpečnosti. Odvracení kybernetických hrozeb, monitoringu stavu infrastruktury, školení uživatelů a dodržování bezpečnostní pravidel je na obcích věnováno značné úsilí a nemalé finanční prostředky.

Přestože se obecně jedná o náročné záležitosti nejen z pohledu bezpečnosti, ale i z pohledu kvalitní a zabezpečené komunikace s občany, daří se výše uvedené rozvojové trendy v obcích postupně realizovat, což veřejnou správu v oblasti eGovernmentu (elektronické vládnutí) zařadilo v roce 2020 na 17. místo v žebříčku členských států EU.

1.1 SWOT z hlediska SMART přístupů v dané oblasti

Obce se v současné době v oblasti SMART digitalizace ICT předně zaměřují na zkvalitňování poskytovaných služeb občanům, aby byly komfortnější, nenutily občana fyzicky docházet na úřad, využívaly se elektronické nástroje pro řešení životních situací a využívaly se informace o občanovi, které byly dříve pořízeny na základě ověření jeho identity. Současně s tímto nárůstem je potřeba klást veliký důraz na zajištění kybernetické bezpečnosti těchto nástrojů a ochranu před zneužitím.

1.1.1 Silné stránky

- Zjednodušení poskytování služeb veřejné správy občanovi;
- ověření identity občana prostřednictvím různých nástrojů;
- řada využitelných zkušeností plynoucích z již realizovaných řešení;
- zvýšení komfortu občanů, kteří mohou své záležitosti řešit dálkově;
- informace a notifikace o průběhu řešení požadavku občana;
- realizace v této oblasti je finančně podporována řadou dotačních zdrojů.

1.1.2 Slabé stránky

- Finančně a technologicky náročná realizace;
- implementace těchto nástrojů je často předmětem osobní snahy a entuziasmu několika pracovníků úřadu spíše než systematickou strategií;
- nedůvěra v tyto technologie, převážně u starších občanů, kteří preferují osobní kontakt;
- neopodstatněný pocit, že pro zajištění řádného provozu je potřeba mít na úřadě ICT specialistu;
- obava z nehospodárně využitých finančních prostředků;
- nízká úroveň bezpečnosti technologií pro SMART řešení plynoucí často ze snahy o co nejnižší cenu;
- používání konfigurace nastavené výrobcem bez přizpůsobení konkrétnímu řešení a bez průběžného reflektování nově se objevujících hrozeb;
- nízké povědomí o nutnosti zavedení přiměřené úrovně systému řízení kontinuity činností (posloupnost činností při řešení technického problému);
- Neochota odpovědných i výkonných pracovníků ve veřejné správě změnit myšlení/přístup při změnách procesů.

1.1.3 Příležitosti

- Zkvalitnění života občanů v obcích;

- umožnění, aby se občané podíleli na rozvoji služeb poskytovaných obcí;
- efektivní oboustranná komunikace s občany;
- modernizace obce a jejího fungování;
- požadavky občanů, hlavně z řad mladé generace;
- využití moderních technologií;
- zvýšení prestiže obce a veřejné správy vůbec v povědomí občanů.

1.1.4 Hrozby

- Změna strategie rozvoje obce po komunálních volbách;
- vendor lock-in při řešení od jednoho dodavatele;
- ztráta odborných znalostí (know-how) při odchodu klíčových pracovníků;
- zneužití či zcizení dat způsobené kybernetickým útokem;
- omezení nebo zastavení chodu úřadu bezpečnostním nebo provozním incidentem a tím i snížení jeho důvěryhodnost v očích občanů, kdy doba obnovení činností je silně závislá na kvalitě nastavení systému řízení kontinuity činností;
- výpadek poskytování služeb z důvodů provozních i bezpečnostních může vést k omezení nebo zastavení plnění zákonných nebo smluvních povinností
- únik nebo krádež osobních údajů ze systémů veřejné správy, ale i informací ze SMART řešení. To může mj. vést k jejich zneužití ze strany kybergangsterů, například využitím informací ze SMART metrů k profilování chování domácností a určení vhodného času k jejich vykradení.

1.2 Shrnutí – základní specifika současného stavu v ČR

Česká republika se od vstupu do Evropské unie zaměřuje na zavádění elektronických informačních technologií do systému fungování veřejné správy, což je obecně shrnuto pojmem e-Government. V současnosti je orgány veřejné moci využíván ISZR – Informační systém základních registrů, KIVS – Komunikační infrastruktura veřejné správy, ISDS – Informační systém datových schránek, CMS – Centrální místo služeb a řada dalších nástrojů a služeb, s jejichž podporou by veřejná správa již nemohla fungovat. Obdobně občané z nástrojů e-Governmentu využívají služby Czech POINT a Portál občana, webovou aplikaci Nahlížení do katastrů nemovitostí a další elektronické nástroje. Bezpečný přístup k těmto službám probíhá přes ověřování identity občana, jehož využívání má od počátku roku 2021 strmý nárůst, díky akceptování ověření občana prostřednictvím bankovní identity (tzv. Bank-ID) neboli jeho ověřením přes elektronické bankovní služby. Z uvedeného shrnutí je zřejmé, že rozvoj SMART řešení v oblasti digitální transformace veřejné správy se dotýká všech subjektů veřejné správy a všech občanů, proto by se i obce samy měly věnovat jejich rozvoji na lokální úrovni. Je nutno si uvědomit, že zavedení nových technologií do prostředí veřejné správy musí být doprovázeno změnou procesů a také změnou myšlení lidí, kteří nové procesy s podporou nových technologií budou realizovat.

Priority a cíle

Poskytování bezpečných digitálních služeb orgány veřejné moci široké veřejnosti, je pro fungování a konkurence schopnost veřejné správy v budoucích letech nezbytné. Hlavně mladá generace požaduje řešení úkonů, životních situací a svých potřeb se subjekty veřejné správy prostřednictvím mobilních aplikací. Tyto požadavky budou

klást na orgány veřejné moci úkoly, týkající se pořízení a provozování SMART řešení, které zjednoduší komunikaci občan – úřad, které zajistí informování občanů o stavu řešení jejich záležitostí, o aktuálním dění v jejich okolí, o stavu splnění jejich povinností (např. úhradě poplatků či pokut), o stavu bezpečnosti školy, kterou navštěvují jejich děti, o kvalitě ovzduší, o hygienických opatřeních, o kulturních a sportovních akcích a řadě dalších záležitostí, které dnes ani nedohlédneme. Ať už to bude jakýkoliv digitální systém, proces či zdroj potřebných informací, tak je potřeba pro jeho kvalitní fungování zajistit komunikační infrastrukturu (metalickou, optickou či bezdrátovou). Dále pak je nezbytné tyto záležitosti zabezpečit proti neoprávněnému přístupu nezvaných návštěvníků a minimalizovat riziko kybernetických incidentů způsobených ať už cíleným nebo nahodilým kybernetickým útokem. Obdobně je tomu u nastupujících SMART technologií, které využívají například prvků Internetu věcí (IoT), jejich vzájemné komunikace a u nichž se předpokládá, že do 10 let doslova zaplaví svět. Budeme se s nimi setkávat naprosto všude. V práci, v automobilech, ve zdravotnictví, v obchodech, prostě v běžném životě, jako tomu je s rozvojem technologií mobilní komunikace. Je proto nezbytné, aby zástupci všech odvětví, včetně veřejné správy věnovali pozornost jejich zabezpečení proti kybernetickým útokům a proti jejich zneužití. Zvyšující se závislost celé společnosti na informačních a komunikačních technologiích klade zvýšený důraz na jejich zabezpečení ať už z pohledu technologického tak z pohledu povědomí uživatelů o kybernetické a informační bezpečnosti.

Priorita 1: Poskytování kvalitních a bezpečných digitálních služeb

Jedním z možných SMART nástrojů umožňující obousměrnou komunikaci občanů s obcí, je webový nástroj známý pod pojmem Portál, obsluhovaný obcí. Přístup na něj je možný například z webových stránek obce, z Portálu občana Ministerstva vnitra či přímým přístupem přes jeho webovou adresu nebo je také provozován formou mobilní aplikace. Nástroje tohoto typu umožňují občanům komunikovat s úřadem, přihlašovat se a odhlašovat k místním poplatkům, dostávat informace o záležitostech, které je zajímají, jako jsou uzavírky komunikací, odečty vody, termíny jednání zastupitelstva a řadu dalších informací. Prostřednictvím implementované platební brány mohou občané rovnou realizovat platby poplatků. Dále pak vznášet připomínky a návrhy, účastnit se anket, či se přihlašovat na různé akce. Díky dostupnosti takovýchto nástrojů i z mobilních zařízení, mohou občané své potřeby a požadavky řešit komfortně z klidu svého domova či třeba z dovolené. Je jisté, že s uplatňováním Zákona o právu na digitální služby pronikne digitální transformace i do dalších oblastí a služeb, které zatím nejsou na první pohled zřejmé.

Cíl 1: Zkvalitnění a rozšíření poskytovaných digitálních služeb

Vytvořením bezpečného webového portálového řešení obce dojde k lepšímu zpřístupnění služeb, poskytovaných občanům a k navýšení jejich komfortní dostupnosti. Kvalitní digitální transformací procesů, které se za portálovým řešením skrývají, dojde také ke zkvalitnění a zrychlení komunikace s nadřízenými orgány, a ke zlepšení poskytování těchto služeb občanům.

Cíl 2: Zajištění dostupnosti poskytovaných služeb všem věkovým vrstvám obyvatelstva

Díky dostupnosti výpočetních a komunikačních technologií pro širokou veřejnost, se poskytované služby v digitální formě stávají dosažitelné pro všechny věkové skupiny obyvatel, protože dnes už neplatí, že tato technika je výsadou pouze mladších generací. Díky těmto skutečnostem dnes není problém i pro starší občany pracovat s internetovými aplikacemi, sloužícími např. pro nákup zboží, pro objednávání na úřady či k lékařům, pro komunikaci s orgány veřejné správy, a přitom využívat nástroje pro ověření své elektronické identity. Obdobně lze potvrdit, že obec může zajistit vyšší dostupnost svých služeb všem věkovým skupinám občanům právě prostřednictvím bezpečných portálových řešení a překonat jejich nedůvěru k těmto řešením.

Priorita 2: Komunikační infrastruktura

Pro zabezpečení výkonu veřejné správy v obcích a poskytování služeb občanům, je nezbytné mít zajištěny vhodné a dostatečně kapacitní komunikační kanály. Nejedná se pouze o rychlý přístup k internetu, ale také o komunikaci se zřizovanými a založenými právními subjekty obcí, se systémem datových schránek, s centrálním místem služeb (CMS) a pro využívání digitálních služeb poskytovaných státem, souhrnně nazývaných eGovernment (elektronické vládnutí). Pro tyto účely je vhodné i do budoucna uvažovat o komunikační síti obce, která by různé subjekty veřejné správy v obci propojila, zajistila jim dostatečný (vysokokapacitní) přístup k internetu a umožnila napojit různé technologie (kamery, měřiče rychlost, chytré senzory, řadiče světelných křižovatek, elektronické označníky na zastávkách MHD a další) do jedné obecní sítě.

Takováto komunikační infrastruktura může být obcí pronajata nebo v lepším případě vlastněna. V případě pronájmu datových tras je z důvodu velkého zarušení radiových frekvencí vhodné uvažovat o metalických či lepe optických trasách. Tato varianta využívání komunikačních tras je vhodná pro malý počet koncových bodů, nebo pro připojení vzdálených lokalit, kde se pronájem v dlouhodobém pohledu finančně vyplatí, oproti instalaci vlastních tras. Nicméně při pohledu do budoucnosti, s vědomím, že se téměř všechny činnosti fungování společnosti přesunují do digitálního prostoru, tak je vhodnější uvažovat o vybudování komunikační infrastruktury ve vlastnictví obce nebo svazku obcí. Při budování datových sítí se již nevyplatí pokládat metalické kabely, ale s přihlédnutím k téměř neomezené přenosové kapacitě použít pouze optické kabely. Přestože zatím obec nemá uvažované koncové body vybaveny vhodnými komunikačními prvky (přepínač, router, kamera, …), tak je vhodné uložit alespoň ochranné prvky pro optickou síť (HDPE trubky), které je následně možné osadit (zafouknout) optickými kabely, v souladu s tím, jak budou požadavky na komunikaci růst. Pro pokládku ochranných trubek lze využít výkopových prací při liniových stavbách v obci, kdy vstupy do pozemků (většinou chodníků a komunikací) a jejich zábory procházejí schválením rady obce, která může investorovi přiložení těchto prvků dát do podmínek. Vlastní projekt vytvoření obecní sítě by měl probíhat v několika základních krocích:

1. Zpracovat projektový záměr (co se má propojit – objekty, kamery, zabezpečení majetku obce, čidla, informační tabule apod.);

2. uspořádat koordinační jednání se zástupci vlastníků technické infrastruktury a zjistit, jaké investiční akce plánují v následujících 5 letech na území obce;
3. zpracovat projektovou dokumentaci pro územní řízení a pro realizaci stavby;
4. zajistit si územní řízení pro vybudování komunikační infrastruktury;
5. realizovat pokládku ochranných prvků a optické kabeláže, z vlastní a dotačních zdrojů a využívat liniových staveb v obci;
6. zprovoznit optické trasy nákupem potřebných technologických komponent (lze realizovat postupně, dle požadavků a finančních prostředků);
7. zajistit si technickou a servisní podporu pro provoz sítě (vlastními pracovníky či odbornou firmou, nebo vhodnou kombinací);
8. provozovat komunikační infrastrukturu a postupně ji rozvíjet dle potřeb obce či svazku obcí.

Cíl 1 – Zajištění bezpečné komunikace v obci

Cílem vybudování komunikační infrastruktury obce je kromě kvalitního poskytování služeb občanům a subjektům na síť napojených, tak se hlavně jedná o zabezpečení komunikace. Veškerá správa sítě není zajišťována komerčním poskytovatelem, ale o všem si rozhoduje obec či svazek obcí samostatně (jaký subjekt či technologii a kdy připojím, jaké služby budu poskytovat a co za ně budu požadovat). V neposlední řadě kvalitní a bezpečné řešení s důsledným rozdělením do segmentů (podle konkrétní architektury komunikační infrastruktury) napomůže i zajištění kybernetické bezpečnosti, kdy například v případě útoku na jeden segment jsou správným nastavením ostatní segmenty proti tomuto útoku ochráněny.

Cíl 2: Rozvoj komunikační infrastruktury pro kvalitní fungování obce

Komunikační infrastruktura v majetku obce či svazku obcí bude v budoucnu hrát stále větší roli v kvalitě poskytovaných služeb občanům. Díky on-line dostupnosti různých služeb technologií a informací z nich, může obec občanům poskytovat aktuální informace o dění v obci, může upozorňovat na aktuální problémy (dopravní nehody, volné kapacity v očkovacích centrech, absence lékaře apod.), kdy tyto aktuální informace dostává právě ze zdrojů připojených na obecní síť. Jestliže se občané budou na základě takovýchto informací rozhodovat ve svých životních situacích, tak o to důležitější je, aby tyto informace byly důvěryhodné a v odpovídajícím čase dostupné, a proto dobře zabezpečené z pohledu kybernetické a informační bezpečnosti.

Priorita 3: Kybernetická a informační bezpečnost

Zajištění kybernetické a informační bezpečnosti se dnes týká všech občanů. V budoucnu bude na bezpečnost kladen stále větší důraz. Bohužel v řadě případů se v poslední době ukázalo, že obce (velké i malé) nejsou před kybernetickými útoky dostatečně zabezpečeny. Vzhledem k tomu, že kybernetický prostor je stále více využíván a řada věcí a lidí bez něj již jen těžko funguje, tak je nezbytné se i v obcích důsledně zaměřit na zajištění kybernetické a informační bezpečnosti. Každá obec si tuto skutečnost musí uvědomit. Nezáleží na tom, zdali je na úřadě jeden či tři sta počítačů, tiskáren a dalších technologií. Zranitelnosti a kybernetické útoky a z nich

plynoucí incidenty se týkají naprosto všech a je potřeba se této problematice důsledně věnovat.
Každá obec by si měla zpracovat v přiměřené míře analýzu rizik, tzn. rozpoznat a popsat, jaká rizika v souvislosti s využíváním informačních a komunikačních technologií hrozí. Z této analýzy vyplyne mimo jiné, i jak dlouho se bez kterého informačního systému obec obejde a dále také, v jakém pořadí je nutno funkčnost jednotlivých informačních systémů po výpadku obnovovat. Například při výpadku ekonomického informačního systému, bez přístupu k datové schránce, bez přístupu k internetu apod. tato analýza rizik je ideálním podkladem pro definování rozpočtu, protože dokáže poměrně přesně popsat poměr mezi náklady na minimalizaci rizik a proti tomu náklady na odstranění škod, pokud se tato rizika neošetří. Je nutno si při této analýze klást také otázky: Jak jsou zabezpečeny zálohy dat úřadu? Jsou pracovníci úřadu dostatečně obeznámeni s bezpečným používáním těchto technologií, např. zda používají dostatečně bezpečná hesla apod. Tedy jaké je povědomí pracovníků úřadu a právních subjektů obcí zřizovaných a založených o bezpečném chování v kyberprostoru? Těch otázek je samozřejmě více a záleží na znalosti prostředí subjektu, využívaných vazeb, legislativních povinností, smluvních vztahů apod.

Dalším nepříjemným faktorem je výše reputačního rizika. Přesněji řečeno poškozením jména subjektu, díky negativní medializaci takového problému a tím významným snížením důvěry občanů k vedení takovéhoto subjektu a veřejné správě obecně. Média v takovýchto případech vždy pokládají otázku „Kdo za to může?“ Zodpovědným je vždy statutární zástupce obce.

Cíl 1: Zajištění kybernetické bezpečnosti a proaktivní odvracení hrozeb

Pro zabezpečení proti kybernetickým útokům a s nimi spojených možných škod, je potřeba proaktivně a včasně řešit technická a organizační opatření. Jednoduše si lze vzít za příklad doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a v přiměřené míře zavést organizační a technická opatření z toho plynoucí. Například řešit antivirové zabezpečení instalací aktuálních virových bází, obdobně instalovat patche (záplaty) operačních systémů serverů a PC, poskytovaných jejich výrobci, reagovat na varování před útoky vydávaných NÚKIB.

Cíl 2: Zvyšování bezpečnostního povědomí

Neoddělitelnou součástí zajištění kybernetické bezpečnosti je průběžné zvyšování povědomí uživatelů o bezpečnostních rizicích a nástrahách. Je potřeba, aby uživatelé byli průběžně poučováni o tom, že kybernetická rizika se jich také týkají a není to pouze záležitost velkých společností, či bankovních institucí, ale opravdu všech uživatelů a informačních a komunikačních technologií obecně, a to nejen internetu. Obec proto musí zajistit pravidelné školení uživatelů, s minimální frekvencí 1x ročně. Pro zajištění dodržování základních pravidel bezpečnosti je vhodné vytvořit bezpečnostní desatero, které musí znát všichni pracovníci úřadu. Při školení je potřeba informovat a rozebírat bezpečnostní incidenty a jejich dopady, které se již staly a vyvodit z nich ponaučení. Stejně tak by měli být uživatelé informováni o tom co dělat a jak se zachovat, když se stanou obětí útoku či zjistí, že už k útoku došlo. Na toto musí být připraveni nejen jednotliví uživatelé ale i subjekt jako celek. V přiměřené míře musí mít zpracován systém zajištění kontinuity činností, plán obnovy činností po výpadku apod. Nelze se

spoléhat na to, že postupy pro obnovení činností někdo nosí v hlavě. V přiměřené míře musí být toto dokumentováno.

Priorita 4: SMART technologie

Chytré technologie neboli SMART technologie v podobě nejrůznější senzorů, čidel, kamer, detektorů a systémů, které informace z nich zpracovávají a na kterých je často závislé rozhodování při řešení životních situací občanů., se postupně stávají součástí běžného fungování obcí. Přestože jsou tyto technologie stále ještě pro některé obce nové a málo známe, tak existuje řada obcí a jejich právních subjektů, kde je již běžně využívají. Jedná se především o senzory a čidla monitorující kvalitu ovzduší, stav hladin vodních toků, obsazenost parkovišť, zaplněnost odpadových nádob, různé kamerové a bezpečnostní systémy, systémy využívající energetický management ke zlepšení hospodaření obce s energiemi a vodou, k evidenci dětí ve školách, k objednávání na přepážky úřadů či k navigaci občanů na různá místa.

Přínosem těchto technologií pro obec je informování o dění a stavu skutečností v reálném čase. Umožňují reagovat na různé situace, jako je zaplněnost odpadových nádob, unikající vodu ve škole, překročení limitů škodlivin v ovzduší, rostoucí hladinu vodního toku, zvýšení hustoty dopravy způsobené náhlým dopravním omezením a řadu dalších.

Pro přenos takových informací se využívají kromě pevných a bezdrátových (WiFi) sítí dnes sítě internetu věcí (tzv. IoT sítě), které na území České republiky provozují různí poskytovatelé. Jedná se především o společnost Vodafon Czech Republic a.s. provozující síť Nb-IoT (Narrow band), společnost T-mobile Czech Republic, a.s. se sítí Sigfox, či České Radiokomunikace a.s. se sítí LoRaWAN.

Těmito sítěmi se sice přenášejí malé soubory dat, ale vzhledem k tomu, že k přenosu dochází s vysokou četností a z velkého množství zdrojů (senzorů), tak se jedná o tzv. Big data. Ta se následně automaticky zpracovávají v příslušných aplikacích a výstupy z nich se srozumitelně prezentují ve formě grafů, tabulek či v barevné škály (obdoba semaforu), informující o závažnosti monitorovaných skutečností. Takovýto SMART systém dokáže příslušné pracovníky úřadu, či pracovníky servisní podpory informovat (mailem či SMS) o stavu překročení určitých limitů, aby mohli dle nastavených procesů řešit nastalé problémy

Cíl 1 – Implementace SMART technologií

Jedním z přínosů implementace SAMRT technologií v obci je zkvalitnění života občanů. Jedná se o to, že občan to nemusí primárně ani vnímat, neboť to nemusí považovat za něco výjimečného. Jedná se o to, že obec těmito nástroji je schopna řešit včasný výsyp zaplněných kontejnerů, aby občané odpad neodkládali mimo kontejner a vítr ho nerozfoukal, dále aby obec včas reagovala na různá nebezpečí, spojená se vzedmutí hladin vodních toků, námrazy nebezpečných míst na vozovce, zhoršení kvality ovzduší, mohla regulovat intenzitu veřejného osvětlení, zvýšila bezpečnost díky kamerovým systémů či monitoringu provozu na průjezdových komunikacích. Je ovšem řada informací, které jsou využívány přímo občany nejrůznějšími cestami např. informace o obsazenosti parkovišť apod. Zde může dojít ke zfalšování takovéto informace např. nasměrováním velkého množství řidičů na jedno „volné“ parkoviště, což může způsobit chaos. Na otázku „Proč by to dělali“

existuje jednoduchá odpověď „Už to udělali“. Takovýchto příkladů z praxe je mnoho. Proto je důležité, aby takovéto systémy nejen fungovaly, ale fungovaly i bezpečně.

Cíl 2: Zlepšení fungování obce – finanční a kapacitní efektivita

Díky provozovaným SMART technologiím dojde ke zkvalitnění fungování obcí v oblastech energetického managementu, svozu odpadů, finančních úspor při včasnému řešení havarijních situací, zkvalitnění komunikace s občany, poskytováním aktuálních informací občanům a umožnit jim se podílet na rozvoji obce, například formou anket, vznášením podnětů a návrhů do participativního rozpočtu či zpřístupněním video záznamů z jednání rady a zastupitelstva apod.

Seznam zkratek a definic

Zkratky a pojmy:

ICT – informační a komunikační technologie (z anglického Information and Communication Technologies)

Czech POINT – Český Podací Ověřovací Informační Národní Terminál, provozovaný Ministerstvem vnitra České republiky. Jedná se o asistované místo výkonu veřejné správy, poskytující řadu výpisů, dokumentů a dalších služeb

SWOT analýza – je metoda analýzy, popisující silné a slabé stránky, příležitosti a hrozby posuzovaného subjektu, záměru či skutečnosti

ISZR – Informační systém základních registrů, provozovaný Správou základních registrů

KIVS – Komunikační infrastruktura veřejné správy, jedná se o bezpečnou, garantovanou a auditovanou jednotnou datovou síť subjektů veřejné a státní správy ČR

ISDS – Informační systém datových schránek – systém provozovaný Ministerstvem vnitra České republiky a sloužící pro elektronické doručování datových zpráv

CMS – Centrální místo služeb – jedná se o soubor technických a programových prostředků, jehož prostřednictvím jsou poskytovány nebo využívány služby informačních systémů veřejné správy

e-Government – je zkratkou anglického electronic government, tedy elektronické vládnutí a jedná se o poskytování služeb veřejné zprávy elektronickou formou

HDPE trubky – jedná se o ochranné prvky (trubky) vyrobené z polyetylenu s vysokou hustotou, které se používané pro instalaci optických a metalických kabelů

WiFi – je označení pro několik standardů IEEE 802.11, popisujících bezdrátovou komunikaci v počítačových sítích

SMART technologie – jedná se o souhrnný název pro chytré technologie

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

IoT – (anglická zkratka pro internet věcí - Internet of Things) jedná se moderní přístroje ovladatelné na dálku i pomocí internetu

LoRaWAN – komunikační síť sloužící pro přenos dat IoT technologií. V ČR je provozovaná společností České Radiokomunikace a.s.

Sigfox – komunikační síť sloužící pro přenos dat IoT technologií. V ČR je provozovaná společností T-mobile Czech Republic, a.s.

Nb-IoT (Narrow band)) – komunikační síť sloužící pro přenos dat IoT technologií. V ČR je provozovaná společností Vodafone Czech Republic a.s.

Relevantní zdroje informací

Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů