Vysoká škola CEVRO Institut

DIPLOMOVÁ PRÁCE

Bc. Jan Zajíček, DiS

Praha 2022

Vysoká škola CEVRO Institut
Katedra bezpečnostních studií

Některé dopady eGovernmentu v malých obcích ČR

Bc. Jan Zajíček, DiS.

Studijní program:	Veřejná správa
Studijní obor:	Bezpečnostní studia
Vedoucí práce:	Ing. Aleš Špidla

diplomová práce

Praha 2022

Prohlašuji, že jsem diplomovou práci na téma *Některé dopady eGovernmentu v malých obcích ČR* zpracoval samostatně, uvedl v ní všechny použité zdroje a v textu řádně vyznačil jejich použití.

V Praze dne 19. 4. 2022

.....

Jan Zajíček

OSNOVA

Resume

Obecní úřady malých obcí se potýkají s jinými výzvami ve srovnání s velkými úřady. S pohledu eGovernmentu nemá jejich činnost takový dopad jako u centrálních orgánů veřejné moci. V malých obcích je eGovernment redukován na informační systém úřadu. Informační systém takového úřadu musí být chráněn nejenom před externími hrozbami, ale také udržován a zabezpečen poučenou obsluhou. Ochrana digitálních dat je nezbytná pro fungování a rozvoj veřejné správy na místní úrovni. Tato práce identifikuje rizika informačních systémů malé obce a předkládá optimální standard pro fungování eGovernmentu v takové obci. Jsou uvedeny konkrétní doporučení a postupy, která mohou pomoci starostům těchto obcí bezpečně zvládnout digitalizaci na svých úřadech.

Resume

Small municipal authorities face different challenges compared to large ones. From the point of view of eGovernment, their activities do not have the same impact as in the case of central public authorities. In small municipalities, eGovernment is reduced to the office's information system. The information system of such an office must be protected not only from external threats, but also maintained and secured by informed staff. Digital data protection is essential for the functioning and development of public administration at the local level. This work identifies the risks of information systems in a small municipality and presents the optimal standard for the functioning of eGovernment in such a municipality. There are specific recommendations and procedures that can help the mayors of these municipalities to safely manage digitization in their offices.

Klíčová slova

• Veřejná správa, místní samospráva, obecní úřad, eGovernment, informační systém, bezpečnost dat

Key words

• Public administration, local government, municipal office, eGovernment, Information system, data security

Metodika

Metodické postupy diplomové práce se měnily v závislosti na fázi výzkumu předkládaného tématu. V první fázi se jednalo o analýzu dostupných dat sekundární povahy a to studium dostupné odborné literatury. V druhé fázi jsem se zaměřil na získání primárních dat přímo v jednotlivých obcích. Třetí fáze se věnuje vyhodnocení dat a návrhu bezpečnostního standardu pro informační systém malé obce. Je třeba dodat, že eGovernment je rychle se rozvíjející obor. Informace, které byly k dispozici před deseti lety, se stávají v dnešní době už zastaralé především z důvodu nových technologií. K tématu eGovernmentu bylo v České republice vydáno několik publikací, kromě toho vycházejí periodika jako Veřejná správa, Moderní obec či časopis eGovernment.

Ve druhé fázi výzkumu (zjištění skutečného stavu eGovernmentu v malých obcích) byly využity dvě empirické metody - dotazníkové šetření a řízený rozhovor. Dotazníkové šetření bylo prováděno pouze na omezeném vzorku malých obcí Hornolidečska (ve Zlínském kraji). Dotazníky měly za cíl zjistit rozsah služeb a zabezpečení eGovernmentu v těchto obcích. Řízený rozhovor s několika starosty těchto obcí pak mapuje názory vedení obce na elektronizaci veřejné správy a s tím spojená rizika zabezpečení informačního systému obce.

V rámci třetí fáze výzkumu proběhlo kvalitativní vyhodnocení získaných informací. Primární data zjištěná u starostů spolu s odbornou literaturou byla využita k analýze rizik eGovernmentu v malých obcích a k navržení standardu zabezpečení informačního systému. Pro formulaci vlastních závěrů k problematice eGovernmentu na malých obcích bylo použito metody analýzy a syntézy, popřípadě indukce a dedukce. Poslední kapitola této práce shrnuje zjištěné skutečnosti a odpovídá na výzkumnou otázku: Jak optimálně zabezpečit fungování eGovernmentu v malé obci?

Úvod

Nové technologie umožnily propojit svět a nám se otvírají možnosti, o kterých se předcházejícím generacím ani nesnilo. Zavádění nových technologických a komunikačních nástrojů do veřejné správy získalo název eGovernment, elektronické vládnutí. Tento vývoj má podobné rysy jako nástup průmyslové revoluce. Nelze ji zastavit. Proto je třeba se zaměřit na využití pozitivních přínosů, ale zároveň musíme eliminovat negativní dopady tohoto procesu. Vybavuji si onen klasický obraz z filmu Charlieho Chaplina „Moderní doba“ (1936), kde se tovární dělník u pásu snaží držet krok s rychlostí výrobního pásu. Ač se snaží sebevíc, tempu montážního pásu nestačí. Tato analogie s automatizací průmyslové výroby může být i obrazem elektronizace v jeho negativní podobě. Elektronizace ve veřejné správě může vést k rizikům jako je znevýhodnění některých skupin obyvatel, ochromení správy (v důsledku ztráty nebo zneužití dat) nebo ke zneužití dat k totálnímu vládnutí. Na druhou stranu elektronizace veřejné správy přináší zefektivnění práce i poskytovaných služeb veřejné správy. Moderní veřejná správa se bez elektronických nástrojů neobejde. Pro občany je novým benefitem to, že mnohé úkony, které v minulosti vyžadovaly osobní návštěvu úřadu, lze vyřešit z pohodlí domova.

Obecní úřady na všech úrovních se musely technicky a organizačně přizpůsobit novému vývoji informačních technologií. Větší obce postupně rozšiřovaly oddělení informačních technologií na svých radnicích. Malé obce se s novým vývojem musely vyrovnat po svém. Malá obec, jejíž obecní úřad tvoří mnohdy dvě osoby, starosta a účetní obce, má podstatně jiné možnosti. Většinou si odborné služby musí zajistit od externích dodavatelů nebo spoluprací s jinými obcemi. Mám za to, že eGovernmentu na úrovni samospráv se dosud věnovalo málo pozornosti. Nejméně pak malým obcím. Přesto právě takových obcí je v České republice nejvíce.

Alfou a omegou eGovernmentu na obecních úřadech malých obcí je zabezpečený informační systém. Cílem této práce je zmapovat současný stav eGovernmentu v malých obcích a navrhnout jeho optimální zabezpečení. Podle mých zkušeností, mnozí starostové mají jen nejasné představy o tom, co jejich obec v oblasti eGovernmentu využívá nebo může nabídnout svým občanům. Navíc při běžné práci

starosty, který jedná s lidmi především "tváří v tvář", se může agenda eGovernmentu (a jeho zabezpečení) ocitnout na vedlejší koleji. Systém eGovernmentu má své nároky na zabezpečení a obsluhu. eGovernment je jako další dveře do obecního úřadu. To, jak budou tyto dveře zabezpečené a funkční, určuje další důvěru veřejnosti v rozšiřování služeb eGovernmentu.

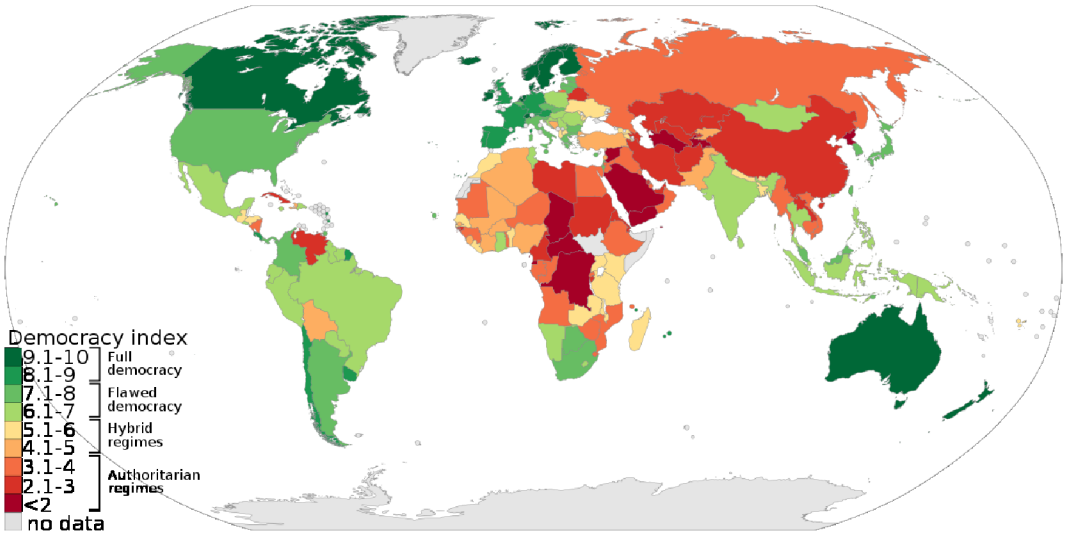
1. Veřejná správa

Veřejná správa nemůže existovat ve vzduchoprázdnu. Předpokladem je existence státu. Stát jako instituce (veřejnoprávní korporace) disponuje autoritou vymáhat zákony, které byly přijaty do jeho právního systému. Stát, kromě státní moci, je definován státním územím a stálým obyvatelstvem. Stát jako politická jednotka musí být uznán mezinárodním společenstvím. Stát je svrchovaný, když není podřízen žádné jiné vnější moci. Podle způsobu vlády rozlišujeme státy demokratické a nedemokratické. V demokratických státech jsou zákony a ústava nadřazeny všem lidem i státním institucím. V nedemokratických státech (diktaturách) existují jedinci nebo skupiny osob, které stojí nad zákonem a nemusí se tedy obávat, že by za své činy byli trestně zodpovědní.

1.1. Dělba moci v demokratickém státě

Vznik demokratických států prošel dlouhým vývojem. Současnou podobu získal v průběhu posledních 200 let. Vyznačuje se rovností před zákonem, důrazem na práva a osobní svobodu jednotlivce a dělbou moci. Již ve středověku mnozí filozofové jako John Locke, Charles Louis Montesquieu nebo James Madison hlásali důležitost dělby moci ve státě. Ten, kdo vytváří zákony, by neměl podle nich řídit stát, natož nestranně vykonávat soud. Cílem oddělení jednotlivých složek moci je snaha zabránit koncentraci moci a její zneužití. (Tak jako se to často dělo u středověkých panovníků). Současné pojetí tak dělí státní moc na moc zákonodárnou, moc výkonnou a moc soudní. Moc zákonodárnou (legislativa) představuje parlament, který schvaluje zákony. Do moci výkonné (exekutiva) patří vláda, která zajišťuje každodenní chod státu. Soudní moc (justice) je oddělena od státu a chráněna před jeho zásahy. Má zajišťovat vládu zákona, rovnost před zákonem a ochranu práv a svobod občanů. Před nespravedlností ze strany státních institucí se v mnohých státech vytvořilo navíc správní soudnictví. Ve světě nacházíme různé variace demokratických států. Můžeme se zajímat také o míře svobody, jaké tyto státy zajišťují. Jak si všímá F. Zakaria, počty demokracií ve světě přibývají, ale osobní svobody jednotlivců nikoliv. „Demokracie sama o sobě nezajišťuje svobodu a lidská práva: "V uplynulých padesáti letech demokracie a

svoboda na Západě splynuly". Jinde ve světě jsou však tyto dvě věci často odděleny. Demokracie vzkvétá, svoboda nikoli.“[1]



Obrázek 1. Státy světa podle Indexu demokracie (rok 2019), Zdroj: BlankMap-World.svg.Data from EIU.com, dostupné z https://commons.wikimedia.org/w/index.php?curid=90686563 [cit. 2022-03-16]

Právní stát

Demokratický stát vznikal tam, kde uspořádání společnosti umožňovalo vznik demokratických institucí. Tyto instituce jednaly v souladu s dosavadním právním vědomím a tento právní rámec se dál kultivoval směrem k ochraně základních lidských svobod.

Z historického hlediska se vyvíjely dvě větve v pojetí právního státu. Kontinentální a anglosaský model. Kontinentální model právního státu počítal s vyškoleným byrokratickým aparátem, rozvojem správního soudnictví a propracovaným systémem správního práva. Anglosaský model neklade takový důraz na byrokracii, ale na úsilí o soulad mezi jednotlivými zájmy ve společnosti, neboli jak poznamenává Hendrych (s. 18): „Na stát (government) se pohlíží jako na nutné zlo, jehož moci mají být jen takové, které jsou absolutně potřebné, a vládní činitelé i státní aparát jsou soustavně drženi "na uzdě" prostředky státního rozpočtu, který schvaluje volený parlament. Právo je samozřejmě i v tomto systému esenciální

[1] ZAKARIA, Fareed. *Budoucnost svobody*. Praha: Academia, 2004. ISBN 80-200-1285-0.

komponentou vládnutí, ale není tak dominantní jako v právním státě (pozn. kontinentálním). Proces vládnutí v tomto systému lze charakterizovat jako trvalé úsilí o získání veřejného souhlasu pro opatření navrhovaná ve veřejném zájmu. S tím souvisí i způsob řešení zájmů různých sociálních skupin, které jsou mnohdy protichůdné a vzájemně nepřátelské. Veřejná správa v takových situacích hraje roli čestného a důvěryhodného rozhodčího vzniklých sporů. Poctivost a nezávislost hry o sektorové zájmy jsou považovány spolu s pragmatismem a flexibilitou za klíčové hodnoty tohoto systému."

Pouze u demokratických států (na rozdíl od autoritativních států) můžeme mluvit o oddělení moci výkonné, zákonodárné a soudní. Také pouze zde můžeme mluvit o veřejné správě jako službě občanům.

Veřejná správa

Obecně správu (řízení, administraci) rozlišujeme na správu soukromých záležitostí a správu veřejných záležitostí. Subjekt soukromé správy může činit vše, co zákon nezakazuje. Naopak subjekty veřejného práva mohou činit jen to, co jim zákon ukládá. Mluvíme o tom, že veřejná správa je vázána zákonem. Soukromou správu kodifikuje soukromé právo, účastníci jsou si rovni. Veřejnou správu kodifikuje veřejné právo a většinou jde o vztahy nadřízenosti a podřízenosti. Jako soukromý občan mám více práv než jako veřejné osoba. (V totalitních státech je to naopak.) V demokratických státech zvolení zástupci veřejné moci slibují dodržování zákonů a ústavy, která je nejvyšší normou ve státě. Slib poslance a senátora podle Ústavy zní: „Slibuji věrnost České republice. Slibuji, že budu zachovávat její Ústavu a zákony. Slibuji na svou čest, že svůj mandát budu vykonávat v zájmu všeho lidu a podle svého nejlepšího vědomí a svědomí.".[2]

Činnost veřejné správy můžeme vymezit pozitivně i negativně. Pozitivní vymezení vypočítává veřejné úkoly, které má veřejná správa zabezpečovat. Veřejné úkoly mohou plnit státní úřady, orgány samosprávy, či dokonce subjekty soukromoprávní. Veřejné úkoly nelze definovat vyčerpávajícím způsobem. Proto

[2] Ústavní zákon č.1/1993 Sb., čl. 23, dostupné z https://www.zakonyprolidi.cz [cit. 2022-03-16]

se činnost veřejné správy definuje také tím, čím se veřejná správa nezabývá. Negativní vymezení veřejné správy můžeme ohraničit jako souhrn činností, které nespadají do oblasti moci zákonodárné ani soudní. Veřejná správa je tedy převážně v rukou exekutivy (vláda a její ministerstva).

Veřejnou správu obvykle rozdělujeme na státní správu a samosprávu. Výkon státní správy uskutečňují ústřední orgány státní správy, ale i ostatní státní orgány a v přenesené působnosti i obce. Jsou tak jakýmisi hybridy, protože kromě své samosprávné autonomie zajišťují na svém území i státní správu. Obce a kraje jsou veřejnoprávní korporace, které vykonávají samosprávu na svém území. Mají právní subjektivitu a mohou spravovat svůj vlastní majetek a uzavírat smlouvy.

„Demokratický právní stát v sobě zahrnuje jako důležitou sociální službu v rámci moci výkonné veřejnou správu, kterou neztotožňuje toliko se státem, ale garantuje ústavou její výkon též v rámci práva na samosprávu.“[3]

1.2. Systém veřejné správy v ČR

Ústavně právní základy organizace veřejné správy ČR nalezneme v ústavním pořádku České republiky, zejména v Ústavě ČR (ústavní zákon č. 1/1993 Sb.) a v Listině základních práv a svobod. Ústavní úprava organizace veřejné správy je obsažena v hlavě třetí Ústavy ČR (státní správa, moc výkonná) a v hlavě sedmé označené pojmem Územní samospráva.

Státní správa je reprezentovaná především vládou ČR, jako vrcholným orgánem výkonné moci. Vláda se skládá z předsedy vlády, místopředsedů vlády a ministrů. Ministři jsou potom zodpovědní za chod jim svěřených resortů. Máme celkem 14 ministerstev: Ministerstvo financí, Ministerstvo zahraničních věcí, Ministerstvo školství, mládeže a tělovýchovy, Ministerstvo kultury, Ministerstvo práce a sociálních věcí, Ministerstvo zdravotnictví, Ministerstvo spravedlnosti, Ministerstvo vnitra, Ministerstvo průmyslu a obchodu, Ministerstvo pro místní rozvoj, Ministerstvo zemědělství, Ministerstvo obrany, Ministerstvo dopravy,

[3] HENDRYCH, Dušan. *Správní věda: teorie veřejné správy*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-561-0., s.19

Ministerstvo životního prostředí. Ministerstva a jiné správní úřady s celostátní působností spolu tvoří organizační soustavu ústřední státní správy.

Na úrovni územní samosprávy existuje v ČR tzv. smíšený model, kdy jednotky územní samosprávy vykonávají vedle vlastní působnosti (samosprávy) i působnost přenesenou (tzn. určitou část státní správy).

Vzhledem k tématu diplomové práce se budu v dalších kapitolách (kap. 2 až 4) věnovat nejprve státní správě na celostátní úrovni. Kapitoly 5 až 7 jsou pak věnovány samosprávě (a to jak vlastní působnosti, tak přenesené působnosti státní správy, kam eGovernment převážně spadá).

Obrázek 2. Správní členění ČR, Mgr. Veronika Doležilová, Pro časopis Řízení školy (říjen 2019), dostupné z www.rizeniskoly.cz [cit. 2022-03-16]

Územní samospráva

V ČR existuje dvoustupňový systém územní samosprávy. První stupeň tvoří obce a druhý stupeň reprezentují kraje. Právním zakotvením organizací krajské samosprávy a jejich kompetencí v zákoně č. 129/2000 Sb. byla završena tzv. první

fáze reformy územní veřejné správy. V rámci tzv. druhé fáze reformy územní veřejné správy došlo v roce 2002 k ukončení činnosti okresních úřadů a jejich činnosti byly přeneseny především na obce s rozšířenou působností a na kraje, popř. na jiné orgány státní správy.

Základní jednotkou územní samosprávy je obec. Obec je veřejnoprávní korporace, tedy právnická osoba, která vykonává správu svého majetku na svém území. Právní předpisy, které regulují postavení obcí v ČR, jejich organizaci a činnost je Ústavní zákon č. 1/1993 Sb. a Zákon č. 128/2000 Sb., o obcích. „Obce se od sebe liší rozsahem výkonu státní správy v přenesené působnosti. Podle rozsahu výkonu státní správy v přenesené působnosti rozlišujeme obce se základním rozsahem přenesené působnosti (všechny obce) a obce s širším rozsahem přenesené působnosti. Jedná se o obce, které vykonávají státní správu v přenesené působnosti i na území druhých obcí, tj. pro obce spadající do jiného správního obvodu. Do této kategorie obcí spadají tzv. pověřené obecní úřady a obce s rozšířenou působností, na které byla převedena většina kompetencí zrušených okresních úřadů.“[4]
Protože téma této práce se vztahuje k malým obcím, budu se dál zabývat jen obcemi prvního stupně. Toto rozdělení kopíruje i velikost obce podle počtu obyvatel. Obce III. stupně jsou do počtu obyvatel největší, obce I. stupně nejmenší. Těchto nejmenších obcí je v ČR nejvíce. Je to dáno historickým vývojem osídlení na našem území. Jak uvádí jedna analýza Českého statistického úřadu: „Sídelní struktura České republiky se vyznačuje značnou roztříštěností, jež je dána dlouhým historickým vývojem sídelní sítě. Typický je velký počet relativně malých obcí. K 1. 3. 2001 existovalo v České republice 6 258 obcí, s celkovým počtem 10 230 060 obyvatel. Průměrná velikost obce v ČR tak činí 1 635 obyvatel. Mediánová velikost obce je však pouhých 382 obyvatel, tzn. plná polovina obcí má méně než 382 obyvatel. Ve velikostních skupinách do 1 000 obyvatel (viz též tabulkové přílohy) se nachází téměř 80 % všech obcí.[5]

[4] PROVAZNÍKOVÁ, Romana. Financování měst, obcí a regionů: teorie a praxe. Praha: Grada, 2007. Finanční řízení. ISBN 978-80-247-2097-5.
[5] Český statistický úřad, dostupné z https://www.czso.cz [cit. 2022-03-16]

1.3. Reformy veřejné správy v ČR po roce 1989

Před r. 1989 existoval systém národních výborů (NV) na jednotlivých územních stupních (místní, okresní, krajské NV) propojených se stranickou organizací Komunistické strany Československa (KSČ). Veřejná správa byla řízena hierarchickým způsobem, tj. shora, v souladu s politikou vlády jediné vedoucí strany (KSČ).[6]

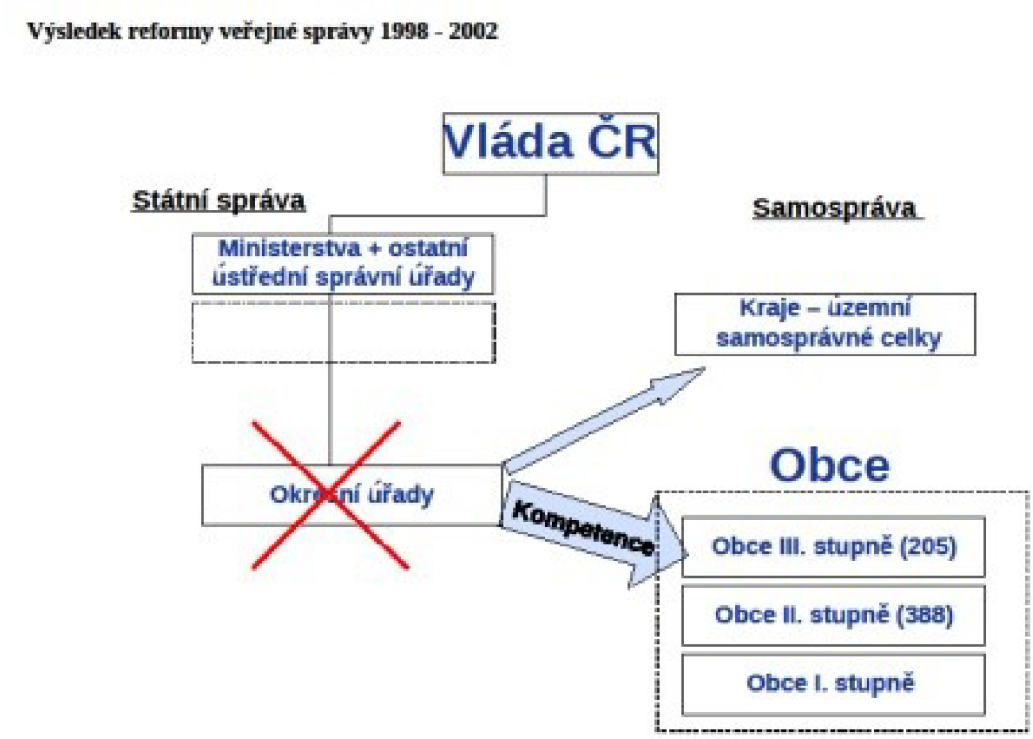
Po roce 1989 byl nejprve obnoven systém samosprávy na místní úrovni (tj. na úrovni obcí), a to v roce 1990. Na úrovni okresů byly okresní národní výbory nahrazeny okresními úřady (zákon z r. 1990). Tyto okresní úřady byly ustaveny jako dekoncentrované orgány státní správy v území. Ředitelé v jejich čele byli jmenováni vládou. Co se týče vyšší úrovně veřejné správy, před r. 1989 existovalo 8 krajů. Ty byly v r. 1990 zrušeny a jejich kompetence byly převedeny na okresní úřady a na příslušná ministerstva. Ministerstva za tím účelem vytvořila řadu detašovaných úřadů v krajských městech.

Schéma veřejné správy po roce 1989

Obrázek 3. Vývoj veřejné správy v ČR po roce 1989, dostupné z https://icv.vlada.cz/cz/proskoly/materialy/politicky-system/system-verejne-spravy-cr-75891/ [cit. 2022-03-16]

[6] Systém veřejné správy v ČR, dostupné z https://icv.vlada.cz/ [cit. 2022-03-16]

Na počátku devadesátých let se vedla diskuze o tom, co nahradí kraje. Nabízely se dvě varianty – zachovat krajské zřízení, či se vrátit ke zřízení zemskému, které fungovalo za 1. republiky. V r. 1991 se nakonec vláda přiklonila k variantě zemského uspořádání. To však nebylo nikdy realizováno. Česká část parlamentu (Česká národní rada) sice již vytvořila příslušné návrhy zákonů, nicméně je v roce 1992 neprojednala z důvodu blížícího se rozpadu československé federace (zánik federace 31. 12. 1992). V Ústavě ČR z r. 1993 je zakotvena existence "vyšších územních samosprávných celků". V té době bylo tedy evidentní, že střední stupeň veřejné správy musí být ještě dotvořen. Již se neuvažovalo o zemském zřízení, ale diskutovala se varianta krajského zřízení. Léta 1993 - 1997 jsou charakterizována hledáním kompromisu o počtu a podobě nového krajského uspořádání. Výsledkem byl zákon z r. 1997, který definoval nové územní členění republiky sestávající ze 14 krajů (Ústecký, Karlovarský, Plzeňský, Středočeský, Liberecký, Pardubický, Královéhradecký, Jihočeský, Moravskoslezský, Olomoucký, Zlínský, Vysočina, Jihomoravský, včetně Hl. městy Prahy jako samostatného kraje). K faktickému naplnění tohoto zákona, respektive k nabytí jeho účinnosti, došlo až 1. ledna 2000.



Obrázek 4. Vývoj veřejné správy v ČR po roce 2000, dostupné z https://icv.vlada.cz/cz/proskoly/materialy/politicky-system/system-verejne-spravy-cr-75891/ [cit. 2022-03-16]

Cílem reforem veřejné správy po roce 1989 bylo zefektivnění správy, její modernizace a přiblížení veřejné správy občanům na principu decentralizace a dekoncentrace. Koncept reformy spočíval ve třech etapách:[7]

1. etapa: vznik krajů jakožto vyšších územně správních celků

Výsledkem této etapy bylo vytvoření 14 krajů, přesněji řečeno 13 krajů a Hl. města Prahy, a zahájení jejich činnosti 1. ledna 2001. Nové krajské zřízení tak začalo fungovat po téměř 11 letech od zrušení toho starého.

2. etapa: zánik okresních úřadů

Největší změna se však udála z hlediska obecního uspořádání. V rámci 2. etapy reformy veřejné správy došlo k rozdělení obcí do tří stupňů na obce I. stupně, obce II. stupně s pověřeným obecním úřadem (388) a obce III. stupně s rozšířenou působností (205). Toto členění zásadním způsobem změnilo systém fungování veřejné správy na nejnižší úrovni. Rozdělení obcí do stupňů bylo úzce spjato se zrušením okresních úřadů (činnost ukončily 31. prosince 2002). Jejich pravomoci převzaly obce III. stupně. (Přestože zanikly okresní úřady, okresy jako správní celky nikoli. To znamená, že některé instituce mají dodnes okresní působnost. Typickým příkladem jsou soudy a policie.) Výsledkem této etapy bylo vytvoření spojeného modelu veřejné správy, který je českým specifikem. Co znamená v praxi? Obce a kraje vykonávají samosprávné funkce a zároveň v tzv. "přenesené působnosti" zabezpečují výkon státní správy. Úředníci obecních a krajských úřadů tak vykonávají současně činnosti v samostatné a přenesené působnosti.

3. etapa: reforma a modernizace ústřední státní správy

Byla chápána jako logický důsledek předchozích etap a měla se týkat centrální úrovně veřejné správy, tedy ústřední státní správy. De facto se nikdy neuskutečnila. Nicméně od roku 2002 jsou zde tendence ústřední státní správu zmodernizovat a v poslední době především zefektivnit. Je nastartována celá řada procesů, které by toho měly docílit, jako eGovernment, zavádění kvality do veřejné správy apod.

---

[7] VOSTRÁ, Lenka, Jarmila ČERMÁKOVÁ a Jiří GROSPIČ, ed. *Reforma veřejné správy v teorii a praxi: problémy reformy veřejné správy v České republice, Maďarské republice, Polské republice a Slovenské republice: sborník z mezinárodní konference: Třešť, 22.-24. října 2003*. Plzeň: Aleš Čeněk, 2004. ISBN 80-86473-71-6. str. 14.

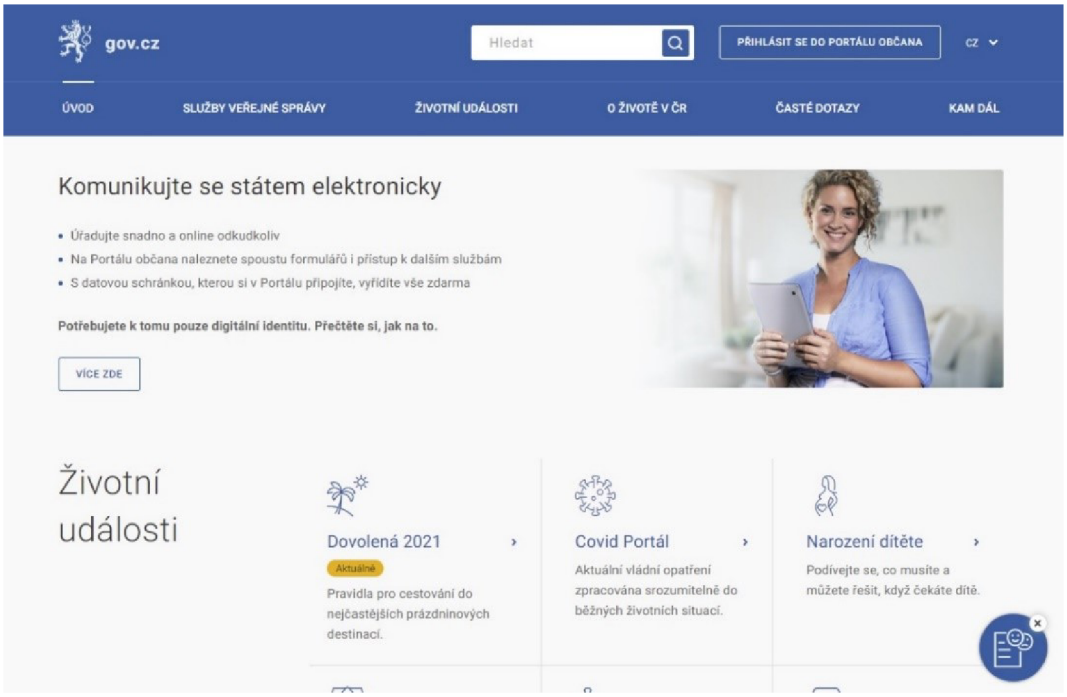
1.4. Zavádění eGovernmentu do veřejné správy v ČR

Po reformě správního uspořádání v roce 2000 (zánik okresních úřadů a vznik krajů) se stává dalším cílem modernizace veřejné správy zavádění koncepce smart administration. Tato koncepce byla definována v dokumentu vlády v roce 2007 pod názvem: "Efektivní veřejná správa a přátelské veřejné služby. Strategie realizace Smart Administration 2007 – 2015". Cílem bylo celkově zkvalitnit služby veřejné správy a zlepšit tak komunikaci mezi úřady a občany. Koncepce byla realizována prostřednictvím projektů, které byly financovány z dotací Evropské unie. Jednalo se především o projekty elektronizace veřejné správy a projekty vzdělávání zaměstnanců veřejné správy. Koordinací projektů bylo pověřeno Ministerstvo vnitra. Podle dokumentu byla veřejná správa v ČR pojata primárně jako služba občanovi. Naplněním této vize bylo zavádění služeb eGovernmentu. Od roku 2008 tak fungují projekty, které se staly základem k rozšíření eGovernmentu ve veřejné správě, ale i jako součást běžného života občana.

Jako první vznikla síť kontaktních míst veřejné správy Czech POINT, která jsou dnes téměř v každé obci. Díky nim mohou občané na jednom místě získat řadu dokumentů a využít služby, kvůli kterým do té doby museli obíhat několik různých úřadů. Byl spuštěn systém datových schránek – nástroj pro zaručenou elektronickou komunikaci se státem, který nahradil klasické posílání obálek s pruhem. Vznikl systém základních registrů, v nichž jsou uloženy aktuálně platné údaje, které už ve většině případů nemusí úředníci opakovaně žádat od občanů. Pro fungování takto složitých a náročných systémů bylo nutné vytvořit masivní a bezpečnou infrastrukturu.

V posledních letech se výrazně usnadnila komunikace občanů s veřejnou správou díky elektronické identitě (identita občana). Elektronická identita je klíčem, který otvírá dveře (portál) k využívání elektronických služeb veřejné správy občany. Je několik způsobů identifikace, jak vydávaných státem, tak soukromoprávními poskytovateli. Od roku 2018 se vydává občanský průkaz s aktivovaným kontaktním elektronickým čipem. Tento nový občanský průkazem slouží i jako identifikační prostředek ve virtuálním světě internetu k prokázání totožnosti v elektronické komunikaci. Původně více portálů (brány k využívání elektronických služeb)

veřejné správy se nyní soustředilo na jednom místě. Tímto centrálním místem se stal Portál veřejné správy na adrese: https://portal.gov.cz/



Obrázek 5. Portál veřejné správy, dostupné z https://portal.gov.cz/ [cit. 2022-03-16]

Na těchto webových stránkách je možné dozvědět se nebo vyřídit:

- Informace o životě a podnikání v České republice (důležité pro cizince nebo imigranty)
- Postupy, jak vyřešit životní události (narození dítěte, změna trvalého pobytu, ztráta zaměstnání apod.)
- Přímo využívat služeb veřejné správy (například vyplnit elektronický formulář příspěvku na péči a odeslat prostřednictvím datové schránky)
- Přihlásit se do Portálu občana a "jít" na úřad konečně on-line (například stáhnout si svůj výpis z rejstříku trestů, podat daňové přiznání nebo zkontrolovat, jaké údaje o mě stát shromažďuje)

Obrázek 6. Portál občana, dostupné z https://portal.gov.cz/ [cit. 2022-03-16]

V roce 2021 vláda schválila Národní plán obnovy ČR, který navazuje na iniciativu EU Nástroj pro oživení a odolnost (Recovery and Resilience Facility, RRF). „Jde o největší nástroj z unijního plánu obnovy Next Generation EU (NGEU), který má členským státům pomoci řešit hospodářské a sociální dopady pandemie koronaviru a zajistit, aby ekonomiky uskutečnily ekologickou a digitální transformaci a staly se udržitelnějšími.“ [8] NPO je pouze jedním z nástrojů, které bude moci ČR využít v příštích letech, NPO tedy nebude pokrývat všechny potřeby země. ČR bude moci kromě NPO využít řadu dalších finančních nástrojů, mj. strukturální fondy, Modernizační fond aj. V NPO je vyčleněno téměř 28 mld. Kč na digitální transformaci země. Má se dále rozvíjet digitální infrastruktura, digitalizace veřejné správy, digitální služby občanům a digitální komerční služby.

[8] Národní plán obnovy, dostupné z https://www.planobnovycr.cz/pilire [cit. 2022-03-16]

2. eGovernment ve státní správě

Současná společnost se velmi dynamicky vyvíjí. Tento vývoj souvisí především s rozvojem informačních technologií. Mluví se o informační společnosti jako dalším stádiu jejího vývoje. Důraz na výrobní prostředky a suroviny nahrazuje důraz na znalosti a soubory využitelných informací. Tato změna důrazu mohla přijít až po vybudování materiálních a logistických struktur. Musel vzniknout surovinový obchod, zpracovatelský průmysl a nové objevy v komunikačních technologiích, abychom jako svět mohli postoupit dál k důrazu na informace, sdílení znalostí a vytváření nových odvětví založených na zpracovávání informací. Kromě dostupnosti osobních počítačů má velký vliv na vývoj společnosti směrem k informační společnosti dostupnost internetu.

Tak jako celá společnost se vyvíjí, tak i veřejná správa absorbuje a využívá elektronické nástroje ve své činnosti. V oblasti veřejné správy mluvíme o zavádění eGovernmentu. Zavádění eGovernmentu je součástí reforem veřejné správy (viz předcházející kapitola). Zavádění eGovernmentu je významným krokem k přerodu státní správy od vrchnostenského pojetí k pojetí státní správy jako služby občanům. Je to ale spojeno s komplikovanými legislativními a technologickými procesy, jež vychází z potřeby zrovnoprávnit elektronické dokumenty s papírovými. Základní požadavky, které jsou na eGovernment kladeny, jsou především bezpečnost a důvěryhodnost.

Definice eGovernmentu

Slovo eGovernment nemá v češtině svůj ekvivalent, jeho doslovný překlad znamená "elektronická vláda". Pojem eGovernment má přesah do různých vědních disciplín jako je informatika, kybernetika, politologie či právo. Spíše než o technický pojem se jedná o politický termín. Používají ho politické strany na ideologické škále zleva doprava. Vzhledem k poměrně dobré dostupnosti internetu u nás, je poptávka po eGovernmentu výrazně tlačena ze strany uživatelů, tedy občanů. Rozvoj eGovernmentu musí být systémově bezpečný. Jinak hrozí nebezpečí ztráty dat a také nebezpečí zneužití těchto dat.

eGovernment někdy bývá zjednodušeně označení jako činnost veřejné správy prostřednictvím elektronických technologií. Lidinský (2008) uvádí definici Organizace spojených národů (dále jen OSN), podle které se jedná o trvalou „povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a efektivních služeb, informací a znalostí. Praktická realizace toho nejlepšího, co může veřejná správa nabídnout.“ A dodává i vlastní definici: „eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb.“[9] Podle Ministerstva vnitra ČR je eGovernment „správa věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější“.[10]

2.1. Vývoj eGovernmentu ve státní správě

Období devadesátých let 20. století můžeme považovat za přípravnou fázi zavádění eGovernmentu do veřejné správy. Je to období nahrazování psacích strojů osobními počítači, vytváření počítačových sítí a rozvoje počítačové gramotnosti. Ke konci devadesátých let pak charakter společnosti ovlivnily další možnosti ICT: mobilní komunikace a rozšíření internetu jako dostupné komunikační platformy a zdrojů informací.

V roce 1996 byl zřízen Úřad pro státní informační systém (ÚSIS). Tento úřad však neměl dostatečně definovány kompetence a pravomoci. I přes problémy spojené s kompetencemi úřad v roce 1999 vypracoval dokument Státní informační politika – cesta k informační společnosti. Jedná se o první dokument, který v podstatě odstartoval zavádění informačních technologií do veřejné správy, a také do české společnosti. Dokument byl schválen v květnu 1999 a představoval vyjádření

[9] LIDINSKÝ, Vít. *EGovernment bezpečně*. Praha: Grada, 2008. ISBN 978-80-247-2462-1.
[10] Co je eGovernment?, dostupné z: https://www.mvcr.cz/ [cit. 2022-03-16]

politické vůle k zavádění moderních technologií a změně společnosti v informační společnost. Vznikly 3 koncepce:

- Informační gramotnost – základním cílem koncepce je rozvoj internetového připojení do škol, a tím podpořit vývoj společnosti směrem k informační
- Elektronický obchod – činit takové kroky, které pomůžou vytvořit vhodné prostředí pro rozvoj elektronických podnikatelských aktivit
- Elektronická veřejná správa

Po zrušení ÚSIS na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy a změně některých dalších zákonů, byly převedeny kompetence tohoto úřadu na nově vzniklý Úřad pro veřejné informační systémy. Mezi základní činnosti, které byly tomuto orgánu svěřeny, lze považovat zefektivnění procesu výměny informací mezi orgány veřejné správy vzájemně, ale také mezi veřejnou správou a občany. Zefektivnění mělo být dosaženo především tím, že se budou využívat k předávání informací data, která jsou již jednou získána, a tím nebude docházet k zatěžování veřejnosti ani orgánů veřejné správy. Hlavní kompetence byly úřadu svěřeny pro oblast nadresortních řešení a také pro oblast sankcionování případného nedodržení platné legislativy v oblasti veřejných informačních systémů. V období let 2003 až 2007 bylo zřízeno Ministerstvo informatiky. Činnosti ministerstva byly vymezené ve čtyřech oblastech (právních předpisech): zákon č. 365/2000 Sb., o informačních systémech veřejné správy, zákon č. 127/2005 Sb., o elektronických komunikacích, zákon č. 29/2000 Sb., o poštovních službách a zákon č. 227/2000 Sb., o elektronickém podpisu. Jako jeden z hlavních přínosů ministerstva lze jmenovat jeho zapojení do legislativní činnosti, kdy byly díky tlakům ze strany ministerstva zakomponovány do nově vznikajících právních předpisů prvky eGovernmentu. Ministerstvo informatiky bylo definitivně zrušeno ke dni 1. 6. 2007 zákonem č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů. Jednotlivé kompetence byly rozděleny následovně:

- **eGovernment má ve správě Ministerstvo vnitra.**
- **Elektronické komunikace připadly Ministerstvu průmyslu a obchodu.**
- **Veřejné dražby má na starosti Ministerstvo pro místní rozvoj.**

Ministerstvo vnitra jako garant eGovernmentu

Ministerstvo vnitra převzalo od zrušeného Ministerstva informatiky i rozpracovaný projekt s názvem eGon. Tento projekt měl za cíl elektronizaci veřejné správy, zmenšení byrokracie a zjednodušení přístupu občanů k veřejné správě. Samo ministerstvo jej představuje na svých webových stránkách takto:[11]

„Moderní, přátelský a efektivní úřad.

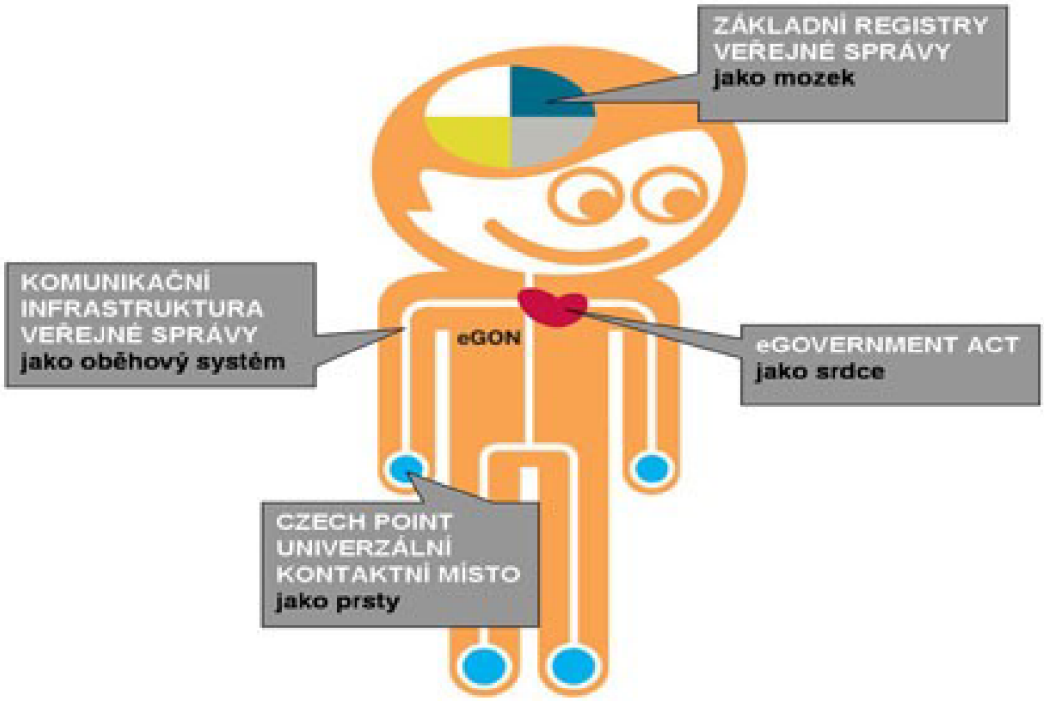
eGON, symbol eGovernmentu, je v přeneseném významu živý organismus, ve kterém vše souvisí se vším a fungování jednotlivých částí se navzájem podmiňuje. Existenci a životní funkce eGONa zajišťují:

- **Mozek: Základní registry veřejné správy (start v roce 2012)**
- **Srdce: Zákon o eGovernmentu (start v roce 2008)**
- **Oběhová soustava: Komunikační infrastruktura veřejné správy (2009)**
- **Prsty: Czech POINT (start v roce 2007)**

S eGONem přichází změna. Končí zbytečné obcházení úřadů, končí pocit beznaděje člověka před kolosem státní byrokracie. Místo toho dochází k zrovnoprávnění elektronických dokumentů s papírovými a vytvoření husté sítě univerzálních kontaktních míst, ze kterých každý může jednoduše elektronicky komunikovat se všemi úřady a institucemi.

eGON je, stejně jako eGovernment, vstřícný, jednoduchý a funkční.“

[11] eGon, dostupné z https://www.mvcr.cz/ [cit. 2022-03-16]



Obrázek 7. eGON, symbol eGovenmentu, dostupné z https://www.zdarns.cz/dokumenty/eGon_brozura_2.pdf [cit. 2022-03-16]

Základní registry veřejné správy

Základní registry jsou centrálně spravované databáze s ověřenými a aktuálními informacemi. Před spuštěním základních registrů si každý úřad vedl svou evidenci, která se nesdílela s jinými úřady. Proto musel občan stále znovu vyplňovat své údaje do formulářů a podpisem stvrdit platnost údajů. „V základních registrech jsou naopak všechny tzv. referenční údaje vždy aktuální a právně závazné. Pokud je úřady pro výkon své agendy potřebují, čerpají je přímo ze základních registrů. Pokud se některý údaj změní, všechny úřady připojené k základním registrům se tuto změnu dozví automaticky. Základní registry jako jeden ze základních pilířů eGovernmentu fungují od roku 2012. Díky nim se zrychlila a zjednodušila řada agend a občané a firmy získali důkladnou kontrolu nad tím, kdo, kdy a proč využívá naše osobní údaje.

Registr osob (správcem je Český statistický úřad) – obsahuje základní identifikační údaje o subjektech, které mají IČO (právnické, podnikající fyzické osoby apod.), jejich provozovnách a statutárních zástupcích.

Registr obyvatel (správcem je Ministerstvo vnitra ČR) – obsahuje referenční údaje o fyzických osobách, které žijí na území ČR (občané ČR i cizinci) a to konkrétně jméno a příjmení, datum a místo narození (a případně úmrtí), adresa místa pobytu, státní občanství, čísla elektronicky čitelných identifikačních dokladů, ID datové schránky.

Registr práv a povinností – obsahuje údaje o vykonávaných agendách a údaje o oprávněních k přístupu k údajům v ostatních registrech.

Registr územní identifikace, adres a nemovitostí (správcem je Český úřad zeměměřický a katastrální) – slouží k evidenci územního členění státu. Vede referenční údaje o stavebních objektech, pozemcích, ulicích, katastrálních územích, atd.“[12]

Obrázek 8. Základní registry (Příručka pro správce AIS), dostupné z https://www.szrcr.cz [cit. 2022-03-16]

[12] Základní registry a Správa zákl. registrů, dostupné z https://www.mvcr.cz/ [cit. 2022-03-16]

Zákon o eGovernmentu

Cílem zákona o eGovernmentu (Zákon č. 300/2008 Sb.) bylo vytvoření optimálních podmínek pro elektronickou komunikaci mezi úřady a občany i mezi úřady samotnými. Rovněž se jím umožní vedení elektronických spisů ve správních řízeních.

Klíčový institut pro provádění elektronických úkonů, tedy pro komunikaci s orgány veřejné moci, představují datové schránky, jejichž informační systém zabezpečuje doručení úředních zpráv v elektronické podobě. Datové schránky umožňují jednoznačně identifikovat příjemce nebo odesilatele. V oblasti elektronické komunikace sehrály roli předskokana elektronické identity.

Druhým klíčovým prvkem zákona o elektronických úkonech je autorizovaná konverze dokumentů, tedy převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo převedení dokumentu obsaženého v datové zprávě do listinného dokumentu a zároveň ověření shody jejich obsahu a připojení ověřovací doložky.

Komunikační infrastruktura veřejné správy

Hlavním cílem Komunikační infrastruktury veřejné správy (KIVS) bylo vytvořit jednotný komunikační rámec pro orgány veřejné správy. První záměry vznikly již za vlády s funkčním obdobím 1998-2002, ale koncepce byla schválena až v roce 2006 a realizace byla zahájena v roce 2007 pod názvem "eGonův oběhový systém" jako projekt Ministerstva vnitra. V odborném jazyce lze říci, že hlavním cílem bylo sjednotit několik datových linek do jedné datové sítě s parametry jako je bezpečnost či vysoký standard nabízených služeb. Očekávaným výsledkem projektu jsou realizované úspory. Komunikační infrastruktura je nezbytnou součástí eGovernmentu, která zajišťuje propojení například mezi orgány veřejné správy a jejími registry, Czech Pointy či digitálními mapami veřejné správy.

Czech POINT

Czech POINT, jinak také Český podací ověřovací informační národní terminál, vznikl již v roce 2007, kdy byly terminály zkušebně spuštěny v několika desítkách

obcí. Hlavním smyslem zřízení Czech POINT bylo zjednodušit komunikaci s úřady a snížit míru byrokracie v České republice, především tím, že vznikne jedno kontaktní místo, které sníží počet nutných návštěv občanů na úřadech. (Místo pěti úřadů navštíví občan pouze jedno místo, kde získá vše potřebné.) V současné době je možné získat na pobočce Czech POINTu [13] například výpisy z centrálních registrů, založit si datovou schránku a také provést autorizovanou konverzi dokumentů z listinné do elektronické formy a naopak.

2.2. Digitalizace služeb veřejné správy

Před digitalizací si každý orgán veřejné moci (OVM) vedl svoji vlastní papírovou kartotéku.[14] Na začátku digitalizace stál digitální podpis a možnost podat žádost elektronicky. OVM začínají využívat své weby jako informační zdroje pro veřejnost. Pracují s elektronickými podatelnami a elektronickými úředními deskami. Zavedení systému datových schránek umožnilo předávání dokumentu mezi úřady navzájem a mezi úřadem a občanem. OVM začínají využívat elektronické spisové služby. Po spuštění Informačního systému základních registrů (ISZR) nastal velký skok. V základních registrech jsou pouze referenční údaje, což znamená, že jsou správné, aktuální a ručí za ně stát.

„Referenční rozhraní veřejné správy umožňuje více subjektům přistupovat k daným datům současně. V rámci tohoto rozhraní lze prostřednictvím Informačního systému základních registrů (ISZR) využívat data ze základních registrů, tj. z Registru obyvatel (ROB), Registru osob (ROS), Registru územní identifikace, adres a nemovitostí (RÚIAN) a Registru práv a povinností (RPP). Ochrana osobních údajů je v základních registrech zajištěna převodníkem agendových identifikátorů fyzických osob (AIFO), díky němuž není možné při znalosti jednoho identifikátoru vyhledávat údaje o fyzické osobě v jiné agendě. Základní registry neslouží k přímému výkonu konkrétní agendy, nýbrž k dodávání garantovaných údajů subjektům, které mají právo údaje pro konkrétní agendy využívat. Jsou tedy nyní

[13] Czech POINT, dostupné z https://www.czechpoint.cz/public/verejnost/sluzby/ [cit. 2022-03-16]

[14] Historie digitalizace služeb,dostupné z https://archi.gov.cz/znalostni_baze:historie_egov [cit. 2022-03-16]

již nezbytným podpůrným nástrojem pro výkon většiny konkrétních agend ve veřejné správě v ČR.“ [15]

V současnosti může občan využívat univerzální kontaktní místa veřejné správy. Buď samoobslužný portál veřejné správy Portál občana (https://obcan.portal.gov.cz/), nebo asistované kontaktní místo Czech POINT (na obecních úřadech, poštách aj.). Občan již nemá povinnost hlásit změny úřadům. Dnes jsme ve fázi propojování datových fondů veřejné správy. Informace (o občanovi), která se objeví v jedné agendě, není vyžadována po občanovi ani v jiných agendách.

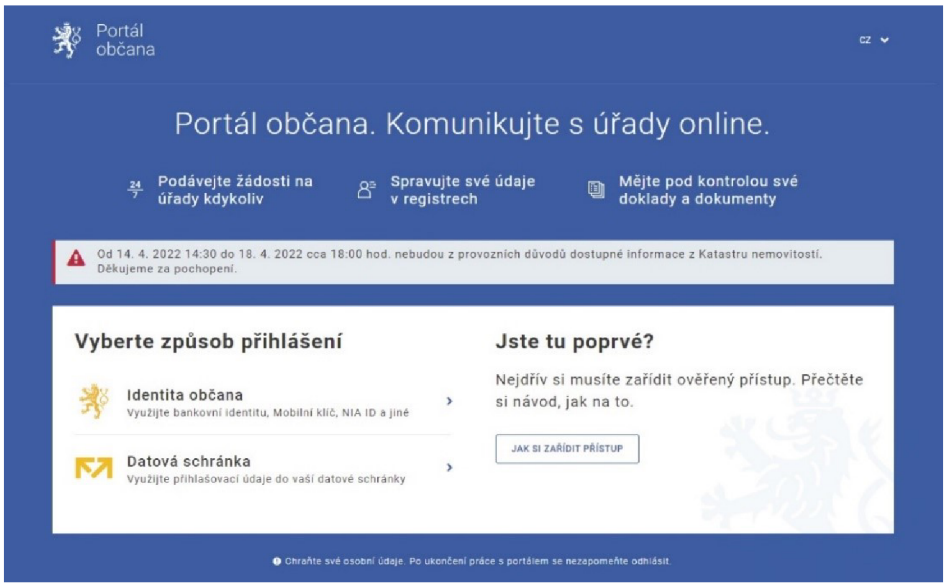
Občan má možnost prostřednictvím elektronické identifikace využívat služeb veřejné správy (agendové služby). Ke každému informačnímu systému (IS) přistupují uživatelé, a proto je nutné ověřit jejich totožnost, tzv. identitu, a nastavit jim práva k jednotlivým úkonům. V oblasti služeb státu je potřeba, aby toto ověření bylo spolehlivé a zaručené na "vysoké" úrovni v souladu s pravidly pro identifikaci klientů veřejné správy. Vždyť jde mnohdy o manipulaci s financemi (daňová přiznání), majetkem (katastr nemovitostí) nebo třeba i s citlivými údaji (zdravotní informace, sociální zabezpečení). K ověření totožnosti slouží elektronické identifikační prostředky, které je možno vnímat jako pomyslný klíč k otevření identifikační brány.[16]

Portál veřejné správy

Portál veřejné správy je komunikační prostředek občana s veřejnou správou. Portál byl vytvořen na základě zákona o veřejných informačních systémech (Zákon č. 365/2000 Sb.) a stal se jedním z nových způsobů komunikace veřejné správy díky rozvoji internetu. Portál zahájil svoji činnost v roce 2003. Podle záměru zákona: „Portálem veřejné správy je informační systém veřejné správy zajišťující přístup k informacím veřejných orgánů a komunikaci s veřejnými orgány.“[17] Přístup k informacím veřejné správy vyrostl od poskytování informací v životních

[15] Identifikace v informačních systémech, dostupné z https://archi.gov.cz [cit. 2022-03-16]
[16] Identita občana, dostupné z https://www.identitaobcana.cz/ [cit. 2022-03-16]
[17] Zákon č. 365/2000 Sb., § 6g, dostupné z https://www.zakonyprolidi.cz [cit. 2022-03-16]

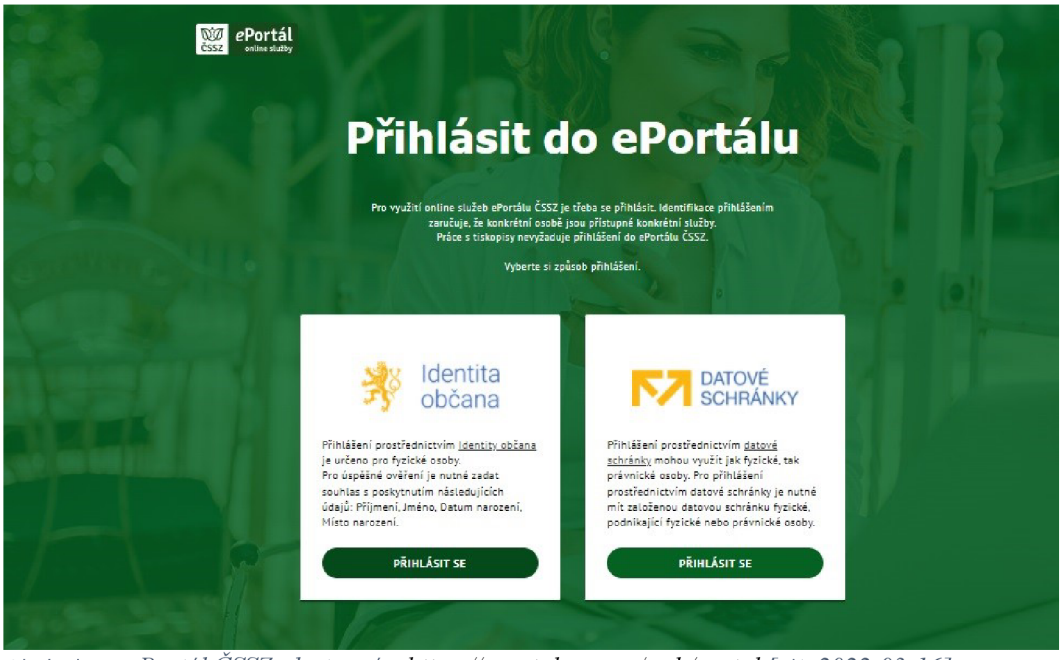
situacích, přes komunikaci s úřady prostřednictvím datových schránek až k elektronické komunikaci s úřady prostřednictvím elektronické identity. Stránky poskytují jak obecné informace o životě v České republice, tak informace o službách veřejné správy. V roce 2018 vznikl **Portál občana**, který byl v roce 2021 integrován do Portálu veřejné správy. Portál občana se stal samoobslužným místem občana směrem k veřejné správě. Umožňuje elektronickou komunikaci s úřady a využívání služeb veřejné správy odkudkoliv na základě elektronické identity. Elektronická (digitální) identita tak umožní (stejně jako občanský průkaz na úřadě) vyřídit úřední záležitosti z pohodlí domova, bez nutnosti chodit na úřad. (https://portal.gov.cz/)



Obrázek 9. Portál občana - přihlášení, dostupné z https://portal.gov.cz/ [cit. 2022-03-16]

Obrázek 10. Identita občana, dostupné z https://portal.gov.cz/ [cit. 2022-03-16]

Po přihlášení do Portálu občana může uživatel využívat on-line služby stejně jako při návštěvě Czech POINTu. Lze také přejít pod svojí identitou do jiných úřadů a vyřizovat tak své záležitosti on-line. Portál občana je tak branou k elektronické komunikaci s úřady.



Obrázek 11. ePortál ČSSZ, dostupné z https://eportal.cssz.cz/web/portal [cit. 2022-03-16]

Elektronická identita občana

„Jako identifikační prostředek lze v současné době využít občanský průkaz s aktivovaným kontaktním elektronickým čipem, NIA ID, moje ID, mobilní klíč eGovermentu, bankovní identitu (bank ID) či první certifikační autoritu. Informační systém datových schránek (ISDS) umožňoval využívat identitní prostor datových schránek k přihlašování do vlastních řešení – typicky portálů. Tento způsob identifikace a autentizace klienta veřejné správy byl umožněn pouze do července 2020, kdy vypršelo přechodné ustanovení zákona č. 250/2017 Sb., které zavedlo povinnost využívat systém Národní identitní autority (NIA). V případě vzdálené identifikace a autentizace prostřednictvím NIA je fyzická osoba jednoznačně identifikována bezvýznamovým směrovým identifikátorem (BSI), který je možné převést prostřednictvím informačního systému základních registrů (ISZR) na agendový identifikátor fyzické osoby (AIFO).“[18]

[18]Identifikace v informačních systémech, dostupné z https://https://archi.gov.cz/ [cit. 2022-03-16]

Zákon o právu na digitální služby

„Digitalizace veřejné správy je v České republice zatím velmi pozvolná, ale postupně nabírá na obrátkách. Významně přispět k tomu může i **zákon o právu na digitální služby** z roku 2020, který dává občanům právo požadovat po státu digitální služby kdykoli, když není pádný důvod pro fyzickou návštěvu úřadu. Navíc občany zbavuje povinnosti poskytovat údaje, kterými již stát disponuje. Tím bude ušetřen čas a úsilí na obou stranách, protože interaktivní formulář předvyplní již dříve sdílená data místo občana.“[19] Zákon o právu na digitální služby 12/2020 Sb. je někdy označován také jako digitální ústava.[20] Zákon stanovuje, že občan může požadovat po státu veškerou komunikaci elektronicky a stát může požadovat po občanovi údaje jen jednou (tedy ty údaje, které občan státu ještě neposkytl). V praxi by to mohlo vypadat tak, že namísto více než 260 různých průkazů a dokladů (občanský průkaz, řidičský průkaz, průkaz pojištěnce, tramvajenka, zbrojní pas, rybářský lístek, …), které v Česku existují, bychom vždy předložili pouze a jen elektronický občanský průkaz uložený třeba v mobilním telefonu, jako to mají v Estonsku, a to by bylo vše. Vyjmuty z povinnosti poskytovat digitální službu byly územní samosprávné celky – obce a kraje, povinnost poskytovat digitální službu jim zůstala pouze pro služby přenesené působnosti.

Přínosy zákona:

- Poskytovatel digitální služby musí uchovávat záznam o digitálním právním jednání občana.
- Pokud není předem zveřejněn elektronický formulář nebo předem stanoven způsob elektronického jednání vůči úřadu, občan má právo učinit podání v jakémkoli formátu poslaném přes datové schránky.
- Po identifikaci občana má tento právo, aby se mu automaticky do interaktivních formulářů vyplnily ty údaje, které už o občanovi stát má.
- Občan má mít právo přístupu ke všem informacím, které o něm stát vede.
- Pokud občan službu v digitální podobě nedostane, může ji vymáhat soudně.

[19] Digitální úřad, dostupné z https://digitalni-urad.cz/#/ [cit. 2022-03-16]
[20] Iniciativa 202020, dostupné z https://www.202020.cz/ [cit. 2022-03-16]

2.3. Koncepční dokumenty eGovernmentu

Iniciačním a koordinačním orgánem vlády ČR pro oblast reformy veřejné správy a eGovernmentu je Rada vlády pro informační společnost (dále RVIS nebo Rada). Vznikla v roce 2014. V roce 2018 došlo ke změně statutu Rady a zřízení funkce vládního zmocněnce pro informační technologie a digitalizaci, který je zároveň předsedou Rady. Nově se tak stává centrálním, koordinačním a řídícím orgánem programu "**Digitální Česko**" Rada vlády pro informační společnost, v čele s vládním zmocněncem pro informační technologie a digitalizaci, ve spolupráci s ministerstvy.

Zastřešující program „Digitální Česko“

„Program "Digitální Česko" je souborem koncepcí zajišťujících předpoklady dlouhodobé prosperity České republiky v prostředí probíhající digitální revoluce. Jeho náplň je možné definovat pojmem: "Strategie koordinované a komplexní digitalizace České republiky 2018+"[21]. "Digitální Česko" zastřešuje tři hlavní pilíře (dílčí koncepce/strategie), které tvoří jeden logický celek s velkým počtem vnitřních vazeb, ale zároveň ve struktuře reflektují zacílení na různé příjemce a rovněž odlišnosti dané současným legislativním vymezením:

- Česko v digitální Evropě (v gesci Úřadu vlády)
- **Informační koncepce České republiky** (v gesci Ministerstva vnitra)
- Digitální ekonomika a společnost (v gesci MPO)“[22]

Informační koncepce České republiky

Na ministerstvu vnitra vznikl odbor Hlavního architekta eGovernmentu (OHA), který má nadresortní působnost a je pověřen koordinací a vedením rozvoje digitalizace veřejné správy. OHA také schvaluje projekty a investice do

[21] Digitální Česko, dostupné z https://www.digitalnicesko.cz/zakladni-informace [cit. 2022-03-16]
[22] Rada vlády pro informační společnost, dostupné z https://www.mvcr.cz [cit. 2022-03-16]

informačních a komunikačních (ICT) systémů veřejné správy, aby byly v souladu s Informační koncepcí ČR.

„Cílem schvalování ICT projektů odborem Hlavního architekta eGovernmentu (OHA) je mj. zefektivnění vynaložených prostředků na ICT, podchycení nekoncepčních projektů a jejich změna ještě před realizační fází, podpora využívání sdílených služeb a postupné utlumování starších IS, které ve své době nebyly koordinovány a principy eGovernmentu ani nemohly dodržovat. V rámci schvalování se OHA zaměřuje zejména na klíčové oblasti architektury eGovernmentu a soulad s národními architektonickými dokumenty, což poskytuje nástroj koordinace ICT na úrovni státu.“[23]

Informační koncepce České republiky je koncepcí rozvoje informačních systémů veřejné správy a eGovernmentu. Koncepci zpracovává Ministerstvo vnitra a schvaluje vláda. Koncepce je vypracována na základě ustanovení § 5a, Zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Informační koncepce ČR je závazná pro všechny státní orgány a orgány územních samosprávných celků. Ministerstvo vnitra v souladu s usnesením zajistilo vydání a uveřejnění dokumentů k Informační koncepci ČR (dále jen IKČR) na internetových stránkách. Tyto dokumenty, které jsou souhrnně označovány jako navazující dokumenty IKČR, tvoří:

- Metody řízení ICT veřejné správy ČR
- Slovník pojmů eGovernmentu
- Národní architektonický rámec
- **Národní architektonický plán**
- Rozšiřující znalostní báze

Povinnost zveřejnit tyto materiály do konce září 2019 byla splněna spuštěním internetové stránky https://archi.gov.cz.

V Informační koncepci České republiky najdeme postupy a standardy k rozvoji eGovernmentu. eGovernment je podle tohoto dokumentu: „moderní digitální veřejnou správou, využívající k výkonu svých působností digitální infrastrukturu,

[23] Národní architektonický plán, dostupné z https://archi.gov.cz/start [cit. 2022-03-16]

realizující sadu ICT služeb, které jsou sdílené, vzájemně sladěné, důvěryhodné, propojené, přístupné, bezpečné, dostupné a efektivní.

Posláním eGovernmentu je:

- Pro klienty veřejné správy co nejjednodušším a nejefektivnějším způsobem poskytovat on-line služby, které jim usnadňují jak dosažení jejich práv a nároků, tak splnění jejich povinností a závazků ze vztahu k veřejné správě.
- Pro úředníky veřejné správy poskytovat standardizované, efektivní, optimálně veřejnou správou sdílené elektronické služby nad referenčními/garantovanými daty při výkonu jejich zákonem dané působnosti.

Vrcholovým cílem eGovernmentu v ČR je, aby do konce horizontu plánu této koncepce platilo, že: "Česká republika je jednou z předních zemí v praktickém využívání moderních služeb eGovernmentu, což významně přispívá k přívětivosti a celkové efektivitě výkonu veřejné moci." Tento cíl eGovernmentu v ČR představuje současně vrcholový dlouhodobý cíl Informační koncepce ČR, která jej rozpracovává do navazujících, závazných a měřitelných cílů realizovaných odpovědnými a při dosahování hlavních cílů spolupracujícími orgány veřejné správy. Jeho výsledkovým indikátorem je pozice ČR v žebříčku dle DESI indexu Evropské komise a stav plnění jednotlivých hlavních cílů Informační koncepce ČR.“[24]

Národní architektonický plán

Národní architektonické dokumenty vznikly na základě usnesení vlády ČR ze dne 3. října 2018 k programu "Digitální Česko" a návrhu změn Statutu Rady vlády pro informační společnost. Ministerstvo vnitra v souladu s usnesením zajistilo vydání a uveřejnění dokumentů k Informační koncepci ČR na internetových stránkách. Národní architektonický plán (NAP) popisuje věcný a technologický pohled na propojení systémů veřejné správy s centrálními sdílenými službami eGovernmentu. Dále definuje, co mají správci informačních systémů činit, aby byli v souladu nejen se současným stavem českého eGovernmentu, ale i s jeho plánovaným stavem. V

[24] Informační koncepce ČR, dostupné z https://archi.gov.cz/ikcr [cit. 2022-03-16]

průběhu časového horizontu NAP, tj. v letech 2019 až 2024, mají být stále více prosazovány změny, směřující k cílové vizi eGovernmentu. Vize architektury eGovernmentu, jako elektronizované veřejné správy, představuje cílovou podobu, jak bude eGovernment v ČR vypadat, až se podaří realizovat podstatnou část opatření uvedených v Informační koncepci ČR a v Národním architektonickém plánu. Z pohledu občana bude veřejná správa sjednocována do dvou základních vnímaných oblastí – jako služby státu, dostupné kdekoli (v přímé i přenesené působnosti, zcela bez místní příslušnosti), a služby samosprávy, srozumitelně spojené s místem života a s jeho obcí. Informační systémy veřejné správy se již nebudou navrhovat, implementovat a provozovat jako nedělitelný blok procházející všemi vrstvami architektury (z angl. pojmu Full-Stack), ale budou koncipovány ve vrstvách – všude kde to je možné, se využijí sdílené služby na příslušné vrstvě. Primárně půjde o transformaci dosud roztříštěných a izolovaných informačních systémů veřejné správy (ISVS) do logicky centralizovaných agendových ISVS:

Byznys architektura veřejné správy ČR	
Sdílené obslužné a komunikační kanály VS	Individuální obslužné a komunikační kanály úřadů
Sdílené služby veřejné správy klientům VS	Individuální služby veřejné správy klientům VS
Sdílené podpůrné služby pro výkon VS	Individuální podpůrné služby pro výkon VS
Sdílené služby správy zdrojů VS	Individuální služby správy zdrojů VS
Sdílené provozní služby státu	Individuální provozní služby úřadů
Architektura informačních systémů VS ČR	
Sdílené aplikační komponenty a služby VS	Individuální aplikační komponenty a služby úřadů
Propojený a veřejný datový fond VS	Vlastní datový fond úřadů
IT technologická architektura veřejné správy ČR	
Sdílené technologické a platformové služby VS	Individuální techn. a platformové komponenty úřadů
Komunikační a provozní infrastruktura veřejné správy ČR	
Sdílená komunikační infrastruktura VS	Individuální komunikační infrastruktura úřadů
Sdílená provozní infrastruktura VS	Individuální provozní infrastruktura úřadů

Obrázek 12. Architektonická vize eGovernmentu, dostupné z https://archi.gov.cz [cit. 2022-03-16]

Byznys architektura - vrstva výkonu veřejné správy

„V dalším vývoji eGovernmentu se zavádí transakční samoobsluha pro subjekty práva a její efektivní asistovanou alternativu pro elektronicky handicapované. Součástí této změny bude rychle rostoucí podíl digitálních služeb, které bude moci

klient získat a být obsloužen v univerzálních kontaktních místech, ať již samoobslužných (jako Portál občana) nebo asistovaných (jako Czech POINT, Call-centrum veřejné správy a také univerzální přepážky úřadů územních samospráv). Všechny lokální územní a resortní agendové portály (jako ePortál, Portál farmáře, eAgri, BusinesInfo, EPO, eHealth a eJustice, a další) budou postupně ve federativním uspořádání připojeny k centrálnímu Portálu občana, který tak bude jediným společným vstupním bodem ke všem elektronickým službám veřejné správy v ČR.“ [25] Elektronické služby pro klienty budou vycházet z jednotné a státem garantované elektronické identifikace občanů ČR (Národní identitní autorita – NIA) a identifikací občanů EU (elektronická identita v EU – eIDAS). Důležitou roli ve zvyšování právního povědomí občanů i úředníků sehrají služby eSbírka a eLegislativa, jako jedny z klíčových znalostních systémů eGovernmentu.

Aplikační architektura – vrstva informačních systémů veřejné správy

Do aplikační vrstvy architektury se neřadí pouze jednotlivé informační systémy veřejné správy či agendové informační systémy, ale také provozní informační systémy a veškeré aplikační komponenty, které jsou v úřadu provozovány, nebo na které se úřad jakýmkoliv způsobem integruje.

Aplikační podpora bude realizována tak, aby zajišťovala zveřejňování údajů jako otevřená data. Sjednotí se jak aplikace na podporu klienta (zejména celostátní Portál občana a s ním federalizované portály ústředních správních úřadů a portály územních samospráv), tak aplikace na podporu práce úředníka.

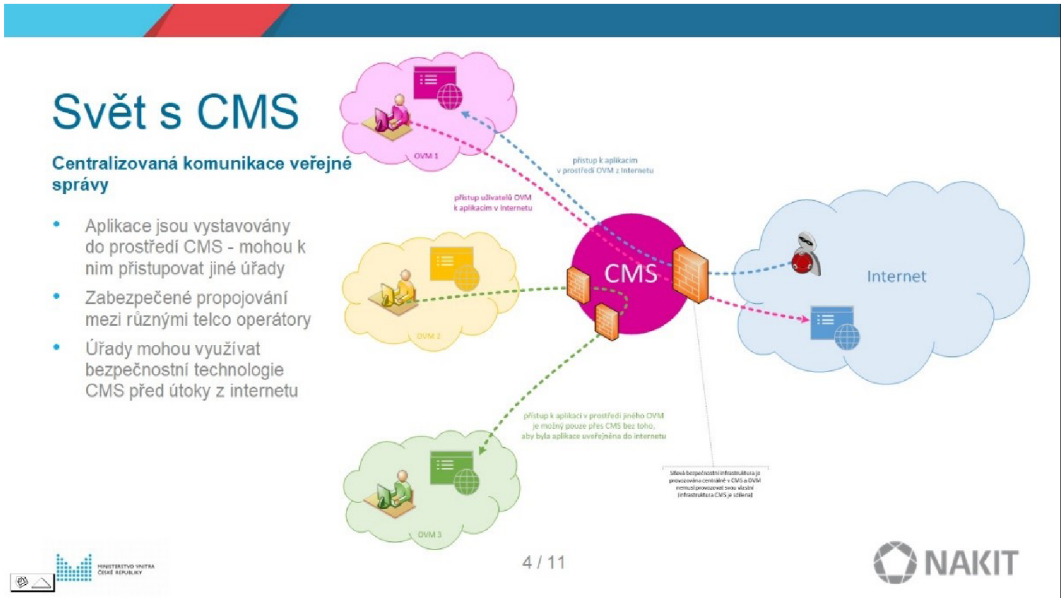
Technologická/platformová architektura – vrstva HW a SW technologií

Zásadním trendem na úrovni technologické vrstvy je využití sdílených platforem výpočetního výkonu a datových úložišť, a to jak on-premise (virtualizace), tak cílově zejména v prostředí **cloudových služeb**. Bude pokračovat budování sítě státních center sdílených služeb a regionálních datových center propojených bezpečnou datovou komunikační infrastrukturou, která budou poskytovat sdílené ICT služby orgánům veřejné správy.

[25] Architektonická vize eGovernmentu ČR, dostupné z https://archi.gov.cz [cit. 2022-03-16]

Komunikační architektura - vrstva komunikační infrastruktury VS

Komunikační vrstva je pro účely architektury veřejné správy ČR speciálně oddělená vrstva, obsahující společné prvky s technologickou vrstvou, avšak zaměřující se na jiný typ služeb s rozdílnou odpovědností. V rámci veřejné správy se na této vrstvě musí vždy objevit datové centrum (fyzická budova), komunikační sítě (internet, komunikační infrastruktura veřejné správy – KIVS) a komunikační uzly (Centrální místa služeb – CMS). CMS poskytují zabezpečené internetové propojení orgánů veřejné správy (OVS), chráněné i proti útokům z internetu.



Obrázek 13. Funkce Centrálních míst služeb (CMS), dostupné z https://www.mvcr.cz/soubor/prezentace-cms2-2017-ok3-ppsx.aspx [cit. 2022-03-16]

eGovernment cloud

Zásadním trendem na úrovni technologické vrstvy je využití sdílených platforem zejména v prostředí cloudových služeb. „Cílem projektu eGovernment Cloud (dále také jako eGC) je zvýšení efektivity, rozsahu poskytovaných služeb, kvality a bezpečnosti a zároveň snížení nákladů provozu informačních systémů a aplikací veřejné správy, a to využíváním sdílených ICT služeb na úrovni infrastruktury, výpočetních platforem a standardizovaných aplikací. Dalším cílem projektu eGC je v maximální míře usnadnit jednotlivým správcům ISVS architektonické,

bezpečnostní, nákupní a projektové procesy využíváním služeb eGC.“[26] Postupně tak bude docházet k využití služeb eGC pro všechny ISVS a provozní informační systémy (migrace do eGC). To umožní úřadům kompletně oddělit "komoditní" komponenty architektury informačních systémů a zaměřit své síly na specifické komponenty, které souvisejí s jejich agendami a kompetencemi.

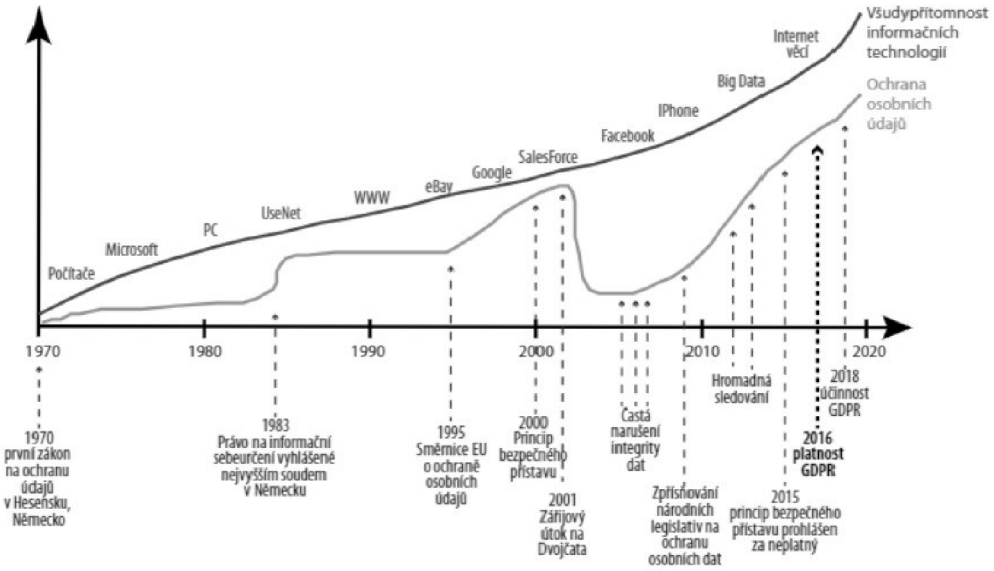
Jaký je rozdíl mezi on-premise infrastrukturou a cloudovými službami? On-premise řešení představuje software či hardware, který je uložen v interní infrastruktuře a prostoru OVS. U on-premise řešení veškerá údržba, aktualizace i zabezpečení spadají do správy OVS samotné, případně OVS najímá externí pracovníky, kteří zajišťují serverovou podporu. Cloud oproti tomu představuje outsourcovanou podobu infrastruktury. Firmy poskytující cloudové služby vlastní datová centra, v nichž pronajímají jednotlivé servery klientům. Klient platí pravidelný poplatek za licenci, která mu umožňuje přístup k datovému úložišti. Tato licence je škálovatelná a její součástí je veškerá serverová podpora. Přístup k datovému úložišti funguje zpravidla přes internet: klient svá data a programy může využívat přes webový prohlížeč na jakémkoliv zařízení.

„Málokteré odvětví se vyznačuje tak jednoznačně rostoucím trendem, jako tomu je u cloudových služeb. V roce 2018 podle výzkumů společnosti IDC celkové využití cloudových služeb překonalo 51 % oproti on-premise. Podle propočtů IDC by navíc tato procentuální převaha měla v roce 2022 přesáhnout 60 %.[27]

[26] eGovernment cloud , dostupné z https://archi.gov.cz/nap:egovernment_cloud [cit. 2022-03-16]
[27] Cloud vs. on-premise: Jaká je budoucnost?, dostupné z https://www.totalservice.cz [cit. 2022-03-16]

3. Rizika eGovernmentu ve státní správě

V předcházející kapitole o eGovernmentu jsem se zaměřil na historii eGovernmentu v ČR, definice a koncepční dokumenty. Zmínil jsem pozitiva eGovernmentu jako je hospodárnost, efektivnost, účelnost (tzv. princip 3E) a přínosy pro občany. V této kapitole uvedu některé slabé stránky a hrozby související se zaváděním eGovernmentu. Bez diskuse nad slabými stránkami a možnými hrozbami se těmto hrozbám prakticky jen přibližujeme a je jen otázkou času, co se kde "pokazí". Hrozby pro eGovernment si můžeme rozdělit na vnější (nezávislé na eGovernmentu) a vnitřní (spojené s činností eGovernmentu).



Obrázek 14. Zaostávání vývoje legislativy za vývojem technologií, Zdroj: Nezmar (2017, s. 15)

Graf výše ukazuje, jak se legislativa (ale i celá veřejná správa) snaží dohnat překotný vývoj informačních technologií. Graf znázorňuje vývoj ICT ve vztahu k ochraně osobních informací. Podobně je to však s ostatními oblastmi legislativy a ochrany uživatele vzhledem k novým trendům a technologiím. Legislativa, ať chceme nebo nechceme, bude pokulhávat za vývojem technologií a snahou některých skupin o jejich zneužití. Podívejme se na možné hrozby, které mohou narušit vývoj eGovernmentu.

3.1. Vnější hrozby eGovernmentu

Vnější hrozby jsou takové, které nemáme přímo pod kontrolou. Stojí mimo náš systém, který chráníme. Tyto hrozby mohou být různého původu (politického, technického, přírodního, sociálního), který můžeme jen s určitou pravděpodobností predikovat. Můžeme se na tyto jevy jen dostatečně připravit a zvážit jejich dopad.

Politické hrozby

Začněme politickými hrozbami. Za určitých okolností mohou nástroje eGovernmentu sloužit ne všem lidem, ale úzké skupině lidí k prosazení své moci. V důsledku rozvoje eGovernmentu se koncentrují informace o jakémkoliv subjektu do centrálního úložiště. I přes legislativní ochranu osobních údajů a rozdělení registrů tak, aby se údaje o subjektu neshromažďovaly na jednom místě, existuje nebezpečí, že státní moc využije údaje o lidech k omezení jejich svobod.

Vezměme si dvě nejčastěji zmiňované dystopie. Dystopie je pesimistická vize společnosti, opak utopie[28] (obraz dokonalé společnosti, ve které lidé navzájem dobře spolupracují a jsou šťastní). Můžeme srovnat pochmurné vize George Orwella popsané v románu 1984 a Aldouxe Huxleyho v románu Konec civilizace. Orwellovská vize se již několikrát naplnila v totalitních ideologiích dvacátého století, v jednadvacátém století přežívají tyto obrazy v Korejské lidové republice, Kubě a Čínské lidové republice. V Číně například existuje státní kreditní systém, který každého vyhodnocuje podle bodovacího skóre.[29]

„Podstatou systému je vytvoření osobního kreditu každého občana, který se pak bude zvyšovat nebo snižovat podle jeho společenského chování. Při zpracovávání mimořádně velkého objemu dat se využívají technologie pro analýzu velkých dat. Přesná metodika výpočtu ani jednotlivé aspekty, které vstupují do hodnocení, nejsou známy. Podle medializovaných informací se kredit bude upravovat na základě:

- Dodržování legislativy (snížení v případě dopravních přestupků, jízdy na černo nebo kouření na zakázaných místech)

[28] Utopie, dostupné z https://encyklopedie.soc.cas.cz/w/Utopie [cit. 2022-03-16]
[29] Čína zavádí sociální kreditní systém, dostupné z https://www.businessinfo.cz [cit. 2022-03-16]

- Ekonomického chování (úprava podle struktury nákupů a řádného placení účtů a daní)
- Sociálního chování (úprava v závislosti od kreditu lidí, s nimiž občan komunikuje, snížení v případě odmítnutí vojenské služby)
- Způsobu využívání digitálních technologií (úprava s přihlédnutím k míře hraní počítačových her, času strávenému na sociálních sítích, sdílení nevhodného obsahu nebo šíření fake news)

Podle různých zpravodajských serverů dosažené "skóre" ovlivní míru sociálního zabezpečení daného obyvatele, dostupnost a podmínky úvěrových finančních produktů (úvěr, hypotéka, kreditní karta), úroveň přístupu do stravovacích podniků, kvalitu ubytování a turistických služeb, dostupnost jednotlivých způsobů přepravy nebo rychlost internetového připojení, dále rozhodne například o přístupu k lepšímu vzdělání nebo zaměstnání (manažerské pozice v státních podnicích nebo velkých bankách). Nízký kredit pak může způsobit i úplné zamezení přístupu k některým službám – například s platností od 1. května 2018 ztratilo 9 milionů občanů (Číny) možnost zakoupit si letenky na vnitrostátní lety a 3 miliony možnost cestovat v obchodní třídě ve vlacích, a to po dobu až jednoho roku.“[30]

Jinou verzi pochmurné budoucnosti představil Huxley v knize Konec civilizace. Huxly si dopisoval s Orwellem a četl i jeho knihu 1984. Orwellovu vizi budoucnosti odmítl s tím, že mocní si najdou jiné nástroje k podmanění lidí, bez mučení a nátlaku. Huxly předestřel společnost budoucnosti jako masy lidí ovládané svými požitky. „Konec civilizace je varováním před otupělostí západní civilizace, ve které jsou lidé pro své pohodlí ochotni obětovat nejen svou svobodu ale i úplný smysl své existence, jež je degradován na život kurů na hnojišti, byť s tolik zrním, slepicemi/kohouty, co trávící potažmo pohlavní orgány zvládnou. Za pomoci vsugerovaných hesel a pouček typu: "každý je dnes šťastný" či "neodkládej na zítřek zábavu, kterou můžeš mít dnes", je smyslem života pracovat, utrácet a konzumovat ať již nezávazný sex, zábavu či zboží, což je dále podporováno drogami, které mají pomoci překonat velmi časté okamžiky prázdnoty a absence

[30] Systém sociálního kreditu, dostupné z https://cs.wikipedia.org [cit. 2022-03-16]

smyslu.“[31] Lidé z takové společnosti nechtějí utéct, nejsou do něčeho nuceni násilím. Jsou udržováni v nevědomí a ve svých závislostech, aby byli ovladatelní. Myslím, že Huxleyho představa je blíž dnešnímu stavu západní společnosti. Pravda se nezakazuje, ale je rozředěna takovým množstvím informací (dostupném na internetu), že si každý může poskládat "svou pravdu".

A co taková doba pandemie. Jaké ta může dát do rukou mocných páky, aby své občany přiměla k poslušnosti! V České republice byl nouzový stav zneužit k vydávání protiprávních nařízení ze strany Ministerstva zdravotnictví za Babišovy vlády. Další kontroverzní kapitolou je povinné očkování a rozdělování lidí ve společnosti na očkované a neočkované. Očkovaní s právy a neočkovaní bez práv (na vzdělání, na práci, na další služby…). Ostatně střet různých názorových proudů provázel společnost celou covidovou dobou a vytvářel rozdělení společnosti. V době pandemie zesílila moc státu a zmenšily se práva občanů. To, že Venezuela, Čína nebo Rusko používají vůči kritikům brutální metody, neznamená, že demokratické země nemají podobné tendence, byť v "měkčím" provedení.

„Pandemie posiluje závislost společnosti na digitálních technologiích v době, kdy je internet stále méně a méně svobodný,“ [32] píše prezident neziskové organizace Freedom House Michael Abramowitz. „Bez odpovídající ochrany soukromí a příslušných zákonů mohou být tyto technologie snadno zneužity pro politickou represi. Historie ukazuje, že technologií a zákonů přijatých v době krize je velmi obtížné se zbavit,“ píše spoluautor zprávy Adrian Shahbaz. „Podobně jako tomu bylo po 11. září, budeme na covidovou krizi zpětně pohlížet jako na dobu, kdy vlády získaly nové možnosti, jak kontrolovat populaci.“ A Abramowitz shrnuje: „Zdravotní krize položila základy pro budoucí, dohližitelský stát.“ Prudký rozvoj umělé inteligence, biometrické sledování lidí, aplikace v mobilních telefonech, které sledují kontakty a dodržování karantény, cenzura kritických příspěvků na internetu a nejasné rozhodování, co je a co není "fake news". Stát využívá moderní technologie a "big-data", aby mohl pohodlně manipulovat veřejností.

[31] Aldous Huxley: Konec civilizace, dostupné z https://www.odaha.com [cit. 2022-03-16]
[32] Ty knihy je potřeba zničit!, dostupné z https://www.seznamzpravy.cz [cit. 2022-03-16]

Závislost na elektřině

Jakákoliv závislost je problém. Závislost znamená nemít možnost volby. Znamená být odkázán na něco, co uvádí celý systém do pohybu. Závislost znamená slabé místo každého konceptu.

Závislost na elektřině je rozhodně klíčová záležitost. Bez stabilní dodávky elektřiny celý koncept eGovernmentu padá. "Systém pohonu" eGovernmentu – energetická soustava je řízena servery, které jsou propojeny mezi sebou prostřednictvím sítě internetu. A i přes technické zabezpečení nelze na 100 % vyloučit možnost výpadku vlivem kybernetického útoku nebo havárie. A čím sofistikovanější systém, tím může být křehčí a náchylnější k různým vlivům. A tím také zranitelnější na kybernetické hrozby. V minulosti jsme byli svědky již několika takových velkých výpadků elektřiny, které dostaly označení blackouty.

Blackout v Severní Americe v srpnu 2003 byl největší výpadek dodávky elektřiny v historii Spojených států amerických, který rozsahem překonal i proslulý blackout v listopadu 1965. V postižené oblasti žije okolo 55 milionů lidí a zahrnuje americké státy Connecticut, Massachusetts, Michigan, New Jersey, New York, Ohio, Pensylvánie, Vermont a kanadskou provincii Ontario. Proud vypadl 14. srpna 2003 v 16:10 místního času. Mnoho lidí uvízlo ve výtazích a soupravách metra, kvůli nefunkčním semaforům se zastavila pouliční doprava, nejezdily elektrifikované vlaky Amtrak a byla uzavřena většina letišť, v horkém počasí nefungovala klimatizace, mobilní telefony byly bez signálu, musela být zrušena řada kulturních a sportovních akcí, věznice a nemocnice jely na nouzové generátory, z bezpečnostních důvodů bylo nařízeno odstavení jaderných elektráren. Docházelo k požárům od svíček, byly zaznamenány i případy rabování, ale nebylo jich tolik jako při předcházejících blackoutech. V New Yorku a dalších velkoměstech byla v té době pouhým okem viditelná Mléčná dráha. Dodávka proudu začala být postupně obnovována od večera 15. srpna, ale omezení provozu elektráren a průmyslových podniků trvala až do 28. srpna. Podle zprávy vyšetřovací komise byla příčinou výpadku programátorská chyba systému EMS v elektrárně firmy FirstEnergy v Eastlake (stát Ohio). Závada nebyla včas oznámena a kvůli špatné komunikaci

nastal dominový efekt. Celková škoda způsobená blackoutem se odhaduje na šest miliard dolarů. [33]

Nestabilitu elektrické rozvodné soustavy bude způsobovat i rozvoj zelené energie, tedy velké kolísání výkonu slunečních a větrných elektráren. Rozvodné soustavy na tak velké kolísání nejsou připravené. Jižní Evropě hrozil masivní výpadek elektrického proudu v lednu 2021. Porucha se rozšířila kaskádovitě z Chorvatska, Srbska a Rumunska. Jižní Evropu museli zachraňovat jaderné a uhelné elektrárny v severní Evropě.[34]

Riziko blackoutu nebývale vzrůstá v současném světě. Na vině jsou tři faktory. Prvním faktorem je nárůst hackerských útoků a kybernetických útoků podporovaných některými státy usilující o narušení západních demokracií (Rusko, Čína). Druhým faktorem je přírodní katastrofa. Tento faktor nelze zcela předvídat a nemůžeme ho ovládat. Můžeme se jen do jisté míry na tuto situaci připravit a počítat s ní v krizových plánech. Přírodní katastrofy jsou navíc v budoucnosti pravděpodobnější v důsledku změn v klimatu. Posledním faktorem, který zvyšuje riziko blackoutu je rozvoj "zelené energie".

Kybernetické hrozby

Kybernetické útoky na veřejnou správu (nemocnice, úřady, ostatní instituce) byly dostatečně popsány v tisku. Do médií se však dostane jen zlomek kybernetických útoků, zejména z oblasti soukromé sféry. Důvod je nasnadě. Firma, která přizná, že byly nabourány její bezpečnostní systémy, zároveň odkrývá, že tyto systémy byly nedostatečně ochráněny. Může to vést ke ztrátě důvěry ~~u~~ napadené firmy. Navíc mohlo dojít i k úniku důležitých informací ze systému (obchodní kontakty, zpracovávané technologie, pracovní postupy, osobní údaje zaměstnanců, obchodních partnerů atd.). Útočníci se často snaží využít svého útoku k vymáhání finančních částek na napadené firmě. Oblíbený je útok pomocí vyděračského software ransomware, který způsobí zašifrování souborů na napadeném počítači (nebo serveru). Takovým útokům čelily mnohé zahraniční i české firmy. Nedávným

[33] Blackout v Severní Americe (2003), dostupné z https://cs.wikipedia.org [cit. 2022-03-16]
[34] Evropě hrozil masivní blackout, dostupné z https://www.idnes.cz [cit. 2022-03-16]

(rok 2021) terčem útoku se stal například obchodní řetězec Coop, který kvůli tomu musel ve Švédsku uzavřít asi 500 prodejen. Hackeři požadovali 70 milionů dolarů (asi 1,5 miliardy Kč). Pachatelé zřejmě pronikli do hojně využívaného nástroje od amerického softwarového dodavatele Kaseya, který slouží IT odborníkům ke správě serverů, desktopů, síťových zařízení či tiskáren. Nástroj s názvem VSA pak upravili a zároveň skrze něj spustili vlnu útoků typu ransomware na cíle, které jej využívají.[35]

V průběhu roku 2021 dokonce americký prezident Joe Biden oficiálně telefonoval prezidentu Ruska Vladimíru Putinovi, aby ruský prezident převzal zodpovědnost za hackery a jejich útoky vedené z Ruské federace na americké cíle.[36] Také v České republice se potýkáme s kybernetickými útoky. Nejsmutnější je, že se hackeři neštítí útočit ani na takové cíle, jako jsou nemocnice.

„Policisté zadrželi gang (poznámka: rok 2021), který stojí za hackerskými útoky na OKD a benešovskou nemocnici. Podařilo se jim to při mezinárodní zásahové akci. Informoval o tom Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Skupina hackerů měla své sídlo v polorozbořeném domě, kde proti ní zasahovaly ukrajinské speciální policejní jednotky. Hackeři pomocí speciálních počítačových virů napadali počítače v Evropě i Spojených státech. Za získaná data poté buď požadovali výkupné, nebo je nabízeli jiným skupinám za úplatu.“[37]

Ke ztrátě dat může dojít i chybnou manipulací obsluhy (například otvíráním mailové přílohy, která způsobí infikování počítače). Pojem virus zná většina z nás. Používáme jej k označování všech forem malwaru. Ve skutečnosti se však jedná pouze o jeden konkrétní druh malwaru. Mezi další druhy patří červi, trojské koně či spyware. Každý druh malwaru má v hledáčku něco jiného. Červi se replikují a zpomalují zařízení. Viry infikují počítače, poškozují tamní soubory a pak se šíří dál. Trojské koně vytvářejí v počítači tajná zadní vrátka, jež hackerům umožňují

[35] USA a další země zasáhl masivní kybernetický útok, dostupné z https://www.irozhlas.cz [cit. 2022-03-16]
[36] Biden vyzval v telefonátu Putina, aby zasáhl proti hackerům v Rusku, dostupné z https://www.irozhlas.cz [cit. 2022-03-16]
[37] Policie dopadla skupinu hackerů, která útočila na benešovskou nemocnici a OKD, dostupné z https://ct24.ceskatelevize.cz [cit. 2022-03-16]

zneužít vaše osobní údaje. Existuje řada důvodů, proč kybernetičtí zločinci tyto druhy malwaru vytvářejí a šíří.

„Ransomware WannaCry útočil na sítě přes protokol SMB verze 1, který počítačům pomáhá komunikovat s tiskárnami a jinými síťovými zařízeními. Tato verze protokolu z roku 2003 obsahovala bezpečnostní chybu MS17-010, jež hackerům otevírala zadní vrátka do počítačů. Společnost Microsoft pro podporované verze Windows již v březnu vydala příslušnou opravu. Ti uživatelé, kteří si ji neinstalovali, se záhy pro WannaCry stali snadným cílem. WannaCry (taktéž WanaCrypt0r 2.0 nebo WCry) v počítačích s Windows šifruje soubory, znemožňuje k nim přístup a po uživatelích požaduje, aby do 3 dnů zaplatili výkupné v bitcoinech v hodnotě přibližně 300 USD. Po uplynutí této doby se cena zdvojnásobí. V květnu 2017, kdy byl zaznamenán jeho největší rozmach, napáchal nejvíce útoků v Rusku, v Číně, na Ukrajině, na Tchaj-wanu, v Indii a Brazílii.

Obrázek 15. Postižené země útokem WanaCry, dostupné z https://www.avast.com/cs-cz/c-wannacry?_ga=2.16097141.2118726208.1637661604-15661832.1637661604

WannaCry zaútočil nejen na jednotlivce, ale také na státní organizace, nemocnice, univerzity, železniční společnosti, technologické firmy nebo telekomunikační společnosti ve více než 150 zemích. Mezi jeho oběti patřila britská National Health Service, Deutsche Bahn, španělská Telefónica, FedEx, Hitachi nebo Renault. Odborníci zjistili, že se ransomware WannaCry chová jako červ a používá dva způsoby útoků z uniklého arzenálu NSA (ETERNALBLUE a DOUBLEPULSAR). Také našli důkazy, které jej spojují se severokorejskou skupinou Lazarus. Tito hackeři si nechávají platit výkupné v bitcoinech a v roce 2014 smazali z databáze

Sony Pictures téměř terabajt dat. V roce 2015 dále vytvořili škodlivý backdoor a v roce 2016 se zapojili do kybernetického útoku, v jehož důsledku bangladéšská centrální banka přišla o 81 milionů dolarů.“[38]

Hybridní hrozby

Hybridní hrozby jsou kombinací různých forem působení státních nebo nestátních subjektů s cílem destabilizovat a oslabit protivníka. Kromě již zmíněných kybernetických útoků zde dále patří šíření cizí propagandy prostřednictvím sociálních médií, manipulace s fakty a dezinformace, manifestace ozbrojené síly a zastrašování pomocí teroristických útoků apod. Propaganda využívající moderní formy komunikace prostřednictvím internetu nabourává důvěru lidí ve státní správu. A tím i v eGovernment. Jak píše Alexandra Alvarová v úvodu své knihy Průmysl lži[39]: „Propaganda není jen šíření lží, jak by se mohlo zdát. Šířeni lží a falešných informací, dezinformací a misinformací je samozřejmě temnější součástí této moderní zbraně. Ale propaganda disponuje neuvěřitelně kreativním arzenálem práce s pravdou, ke které přimíchává významy, akcenty, tu a tam drobnou lež, někdy jiné vyznění, správný podtext, mírně manipulovanou fotku - a polopravda už náhle nevypadá tak nesnesitelně hloupě, je z ní kočka, v médiích působí sexy, začíná po ní být poptávka.“ Výsledkem působení propagandy je vnitřně rozdělená společnost neschopná se bránit vnějšímu nepříteli.

Oblasti, ve kterých hybridní kampaně mohou probíhat, jsou označovány zkratkou DIMEFIL a jsou definovány v Auditu národní bezpečnosti (2016):

D) „diplomacie/politika – uplatnění vlivu a vyvíjení nátlaku ústy a činy oficiální politické reprezentace;

I) informace – sdělovací prostředky, sociální sítě a jiné prostředky šíření informací, jejich manipulativní využití, dezinformační kampaň a propaganda;

M) ozbrojené síly – může jít o otevřené použití jako výhružka (demonstrace vojenské přítomnosti a pohotovosti) či přímo bojové použití nebo o různé formy skrytého nasazení jednotlivců, malých skupin a infiltrace napadeného státu s jejich využitím;

---

[38]WannaCry, dostupné z https://www.avast.com [cit. 2022-03-16]

[39] ALVAROVÁ, Alexandra. *Průmysl lži: propaganda, konspirace a dezinformační válka*. Praha: Stanislav Juhaňák - Triton, 2017. ISBN 978-80-7553-492-7.

E) ekonomika – různé formy nátlaku ekonomické povahy (uvalení cla, embarga, odepření dodávek surovin či energie, zákaz používání dopravní nebo přepravní cesty, destabilizace klíčových odvětví, podniků apod.);
F) finančnictví – destabilizace měny, trhu s akciemi a dluhopisy, bankovního sektoru, ovlivňování klíčových finančních institucí;
I) zpravodajství – aktivity zpravodajských služeb, špionáž, získávaní spolupracovníků (zejména státních či politických činitelů) k protistátní činnosti;
L) veřejný pořádek a právní stát – využití různých rozvratných činností útočících na hodnotové, právní a další aspekty společenského uspořádání, např. podněcování nepokojů v napadené zemi s využitím etnických, náboženských či sociálních dělících linií ve společnosti, nebo použití široké škály teroristických útoků a dalších typicky kriminálních metod (např. únosy, vydírání a zastrašování).“[40]
Audit ukázal, že Česká republika v době vydání dokumentu, není dostatečně chráněna před kombinovaným rozvratným působením cizího státu. Příkladem může být zapojení dvou agentů ruské vojenské rozvědky GRU – Anatolij Čepiga a Alexandr Miškina ve výbuchu vojenských skladů ve Vrběticích v roce 2014.[41] Pro stabilitu společnosti je podstatné zamezit šíření ruských dezinformací, které se snaží (a často úspěšně) odklonit důvěru občanů v politický systém naší země. Aktuálně (duben 2022) můžeme sledovat šíření dezinformací (a lží) v souvislosti s ruskou agresí na Ukrajině a zločinech páchaných na okupovaných územích Ukrajiny.

Hrozba nedostupnosti nebo ztráty dat

Mezi další hrozby můžeme zahrnout i ty, které souvisí s fyzicky uloženými daty v datových úložištích. Ať už mluvíme o datech uložených lokálně nebo v cloudu, vždy mají své fyzické umístění. Toto místo se může stát terčem teroristického útoku, místem přírodní katastrofy nebo "jen" místem vzniku požáru. Velká datová centra bývají samozřejmě velice dobře ochráněna proti požáru, mají různé atestace bezpečnosti apod. Přesto může nastat situace, kdy ani to nepomůže. Příkladem může být požár datacentra v budově Alsace Tourisme SBG2 ve Štrasburku 10.

[40] Audit národní bezpečnosti, dostupné z https://www.vlada.cz [cit. 2022-03-16]
[41] Kauza Vrbětice, dostupné z https://cs.wikipedia.org [cit. 2022-03-16]

března 2021. Pravděpodobná příčina požáru? Poškození optického vedení a trafostanice.

Tyto hrozby nabývají na aktuálnosti s rozvojem cloudových služeb (viz kapitola 2.4. oddíl eGovernment cloud). Jak uvádí jeden analytik pro privátní sektor (což platí analogicky i pro veřejný sektor): „Dle posledního výzkumu skutečného stavu informační bezpečnosti v organizacích v ČR, se s výpadkem služeb třetí strany setkalo 70 % organizací, takže se rozhodně nejedná o nějakou hypotetickou hrozbu, a bez ohledu na to, co je příčinou výpadku, je potřeba mít kvalitně připraven a otestován DRP (Disaster Recovery Plan). Mimochodem test plného přerušení skoro nikdo nedělá. Ideálně takový, který vám umožní svůj core business rozjet v jiném datovém centru a u jiného poskytovatele. To znamená, že buď musíte mít někde zálohovaná data a připravenou infrastrukturu, kde budete moci systémy nainstalovat, nakonfigurovat, spustit a data obnovit ze záloh. Anebo pokud je pro vás business čas kritický, tak musíte provozovat ještě jednu instanci s aktuálními daty někde jinde anebo dané řešení postavit jako skutečný heterogenní geo cluster. Ano, pak už ten outsourcing takovéhoto řešení cenově až tak výhodný vůbec nebude.“[42]

Sociální hrozby

V zákoně O právu na digitální službu je zaneseno právo občana požadovat po státní správě (pokud to je možné) digitální službu. S tím, jak se rozšiřuje možnost komunikovat s úřady digitálně, se zároveň mění i způsoby podávání žádostí úřadům. Mnohá podání lze v dnešní době podat pouze elektronicky. Ale co když občan nemá dostatek zkušeností nebo znalostí, aby takové podání udělal? Nenastane vyloučení skupiny obyvatel, které nebudou moci komunikovat s úřady elektronicky? Tvůrci eGovernmentu počítají s postupným seznamováním veřejnosti s elektronickými nástroji a jako záchrana slouží univerzální kontaktní místa (například na každém obecním úřadě) Czech POINTy. I přes snahu o dostupnost digitálních služeb bude přesto ve společnosti stále skupina lidí, kteří si s digitálními službami nebudou vědět rady. Pokud nebude k dispozici nějaká forma sociální asistence, mohou se stát tito lidé odstřiženi od služeb veřejné správy.

[42] Data v cloudu, data v čoudu, dostupné z https://www.cleverandsmart.cz [cit. 2022-03-16]

3.2. Vnitřní hrozby eGovernmentu

Vnitřní hrozby můžeme ovlivnit svými opatřeními a tak je eliminovat. Vnitřní hrozby vznikají uvnitř chráněného systému (ať už vlivem techniky, lidí nebo procesů). Okruh vnitřních hrozeb se liší podle řešeného stupně eGovernmentu. Jiný je u státního eGovernmentu a jiný je na úrovni obce. V každém případě je to oblast, kde provádíme konkrétní bezpečnostní opatření.

Hrozba ztráty dat

Ztráta dat v rámci nějaké organizace je noční můra. I přes vypracovaný systém zálohování může nastat nějaký problém. Jako byla ztráta osobních údajů 46 000 klientů společnosti Zurich Insurence. Stalo se to v okamžiku přenosu dat ze zálohovací pásky do vzdáleného úložiště v Jihoafrické republice.[43] Při ukládání dat do cloudu, tedy přenášení dat na jiné místo prostřednictvím internetu, je důležité, aby byl zabezpečený přenos dat. Standardem je přenos dat zašifrovaně.

Důležitá data organizace mohou být také odcizena fyzicky (děje se tak především vlastním personálem). Asi k nejznámější krádeži dat došlo v roce 2013, kdy bývalý pracovník Národního bezpečnostní agentury USA Edward Snowden vynesl dokumenty a informace, které dokládaly mimo jiné, že americké tajné služby sledují telefonní hovory milionů Američanů. Ač odvolací soudy v USA v roce 2020 rozhodly ve prospěch Snowdena, ten se stále ukrývá v ruském exilu před dalším stíháním ze strany amerických úřadů. Data mohou být odcizena společně s nosičem dat. Nejčastěji bývají ukradeny notebooky s citlivými daty. Jistou ochranou proti zneužití dat z ukradeného notebooku je samozřejmě přístupové heslo do notebooku, nebo také šifrování souborů na harddisku. Jak může být vyčíslena škoda způsobená ztrátou dat, uvádí další příklad. Až na částku mezi 100 a 500 miliony amerických dolarů se vyšplhala náprava všech škod spojená se zneužitím osobních údajů vojenských veteránů ve Spojených státech, včetně dat narození a čísel sociálních

[43] VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-671-6., s.133

pojistek. Data se nacházela na notebooku ukradeném v roce 2006 v domově jednoho ze zaměstnanců vojenské správy.[44]

Porušování bezpečnostních standardů zaměstnanci

Nejčastější příčiny bezpečnostních incidentů mají na starosti zaměstnanci a to nerespektováním bezpečnostních opatření. Způsoby obcházení bezpečnostních opatření mohou být různé: instalace libovolného software na pracovním PC, klikání na podezřelé odkazy v podezřelém mailu, používání cizího paměťového média (např. USB flash disk), apod. Mnohé takové praktiky se dají eliminovat pravidelným školením zaměstnanců. Pomáhá také oficiálně vydaná bezpečnostní politika nebo standard bezpečnosti, který je zveřejněn, popřípadě podepsán zaměstnancem.

[44] VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-671-6., s.170

4. Zabezpečení eGovernmentu ve státní správě

U eGovernmentu ve státní správě se používají příslušné nástroje s celostátní působností. Patří mezi ně legislativa, technické a institucionální zabezpečení a vzdělávací systém. To vše determinuje i eGovernment na lokální úrovni, který bude popsán později. Podívejme se ale nejdříve na tyto celostátní nástroje zaměřené na snížení rizik eGovernmentu.

Legislativa

Legislativa kromě nastolování pravidel je také nositelkou hodnot ve společnosti. V ideálním případě by měla chránit toho, kdo je nějakým způsobem v nevýhodě, nebo je slabší. V oblasti eGovernmentu se tak může ocitnout občan jako ten, který tahá za kratší konec provazu, proto by měl být adekvátně ochráněn. Je několik zákonů, které ten pomyslný konec provazu trochu srovnává. V oblasti eGovernmentu jsou to především tyto zákony:

- Zákon č. 12/2020 Sb., o právu na digitální službu
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- zákon č. 123/1998 Sb., o právu na informace o životním prostředí

Veřejná správa funguje vždy výhradně v mantinelech zákonů a zákonných povinností a používá metody, způsoby a prostředky, které ji zákon přikazuje. Další legislativa k eGovernmentu:

- Zákon č. 111/2009 Sb., o základních registrech
- Zákon č. 250/2017 Sb., o elektronické identifikaci
- Zákon č. 500/2004 Sb., Správní řád
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- zákon č. 123/1998 Sb., o právu na informace o životním prostředí
- Zákon č. 200/1994 Sb., o zeměměřictví
- Zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Instituce

Bezpečnostní instituce zabezpečují chod eGovernmentu. Jednak udržují elektronické komunikace a také chrání kritickou infrastrukturu před kybernetickými hrozbami. Z těchto institucí jmenujme nejdůležitější NAKIT a NÚKIB. V oblasti kybernetické bezpečnosti je nezastupitelná Bezpečnostní informační služba. Ochranou osobních dat uživatelů v kyberprostoru (nejenom) má na starosti Úřad pro ochranu osobních údajů.

Národní agentura pro komunikační a informační technologie, s. p.[45] byla založena 1. února 2016 jako servisní organizace ministerstva vnitra České republiky. NAKIT je strategický partner státu zajišťující komunikační a informační služby pro záchranné a bezpečnostní složky a veřejnou správu. Poskytuje služby v oblasti informačních a komunikačních technologií s využitím více než 40 regionálních pracovišť. Její služby pokrývají tři oblasti: infrastrukturní služby, aplikační služby a kybernetickou bezpečnost. Infrastrukturní službou je vše, co souvisí s návrhem, realizací a provozem technických prostředků pro zajištění chodu komunikačních a informačních technologií, zejména pak přenosové sítě, mobilní sítě, datová centra a IT infrastruktura.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)[46] je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na

[45] NAKIT, dostupné z https://nakit.cz/o-agenture-nakit/ [cit. 2022-03-16]
[46] NUKIB, dostupné z https://www.nukib.cz/cs/ [cit. 2022-03-16]

starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Ředitel Úřadu se též pravidelně účastní jednání Bezpečnostní rady státu (BRS) a je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem BRS pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky.

Bezpečnostní informační služba je zpravodajská instituce českého státu, která působí uvnitř jeho území. Službu řídí a kontroluje vláda ČR a její fungování upravuje zákon o Bezpečnostní informační službě (č. 154/1994 Sb.).

Oblasti, kterými se BIS zabývá, vymezuje zákon o zpravodajských službách ČR (č. 153/1994 Sb.). Zjištěné informace BIS předává prezidentu republiky, vládě (předsedovi vlády a jednotlivým ministrům), státním a policejním orgánům. Jako instituce je přísně apolitická, nemá represivní pravomoc – nemůže zadržet, zatýkat ani vyslýchat. „BIS se v rámci své působnosti zabývá jevy a aktivitami, které by mohly mít dopad na bezpečnostní zájmy ČR nebo představovat reálné či potenciální hrozby pro komunikační infrastrukturu a její uživatele a věnuje se tématům z oblasti kybernetické bezpečnosti. BIS se zabývá např. šetřením nejrůznějších druhů elektronických útoků s dopadem na chráněné zájmy ČR, a dále shromažďováním a analýzou informací o reálných či potenciálních hrozbách a rizicích souvisejících s provozováním strategických informačních a komunikačních systémů, jejichž zničení či narušení by mohlo mít vážný dopad na bezpečnost či ekonomické zájmy ČR. Jedná se zejména o systémy úřadů a institucí veřejné správy či dalších právnických osob, včetně soukromoprávní sféry, u kterých se předpokládá zvýšená ochrana v souvislosti s jejich významem či ve vazbě na jejich potenciální zařazení mezi subjekty kritické infrastruktury ČR. V souvislosti se zajišťováním kybernetické bezpečnosti BIS průběžně prověřuje také různá internetová fóra, jejichž prostřednictvím dochází k nelegálnímu obchodu s osobními údaji osob či jinými citlivými daty, nebo která

případně slouží jako kontaktní místo pro střetávání nabídky a poptávky po různých formách elektronických útoků, nástrojů k jejich provádění atd.“[47]

Úřad pro ochranu osobních údajů (ÚOOÚ)[48] byl s účinností od 1. června 2000 zřízen zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Dne 24. dubna 2019 byl tento právní základ transformován na zákon č. 110/2019 Sb., o zpracování osobních údajů (ZZOÚ).

Posláním Úřadu je napravit chybné procedury zpracování osobních údajů správci nebo zpracovateli osobních údajů. Nezabývá se proto každým porušením ochrany soukromí; je věcí poškozeného, aby se domohl nápravy žalobou u soudu. Úřad se zabývá nedostatečnou ochranou osobních údajů, která má systémový přesah, tj. z její nápravy bude profitovat větší množství subjektů údajů.

Kromě ochrany osobních údajů plní Úřad další úkoly svěřené mu zákonem. Jedná se například o elektronické identifikátory (podle § 11 zákona č. 111/2009 Sb., o základních registrech), svobodný přístup k informacím (podle § 16b zákona č. 106/1999 Sb., o svobodném přístupu k informacím) nebo elektronické komunikace (podle § 87 odst. 4 zákona č. 127/2005 Sb., o elektronických komunikacích).

Vzdělávání

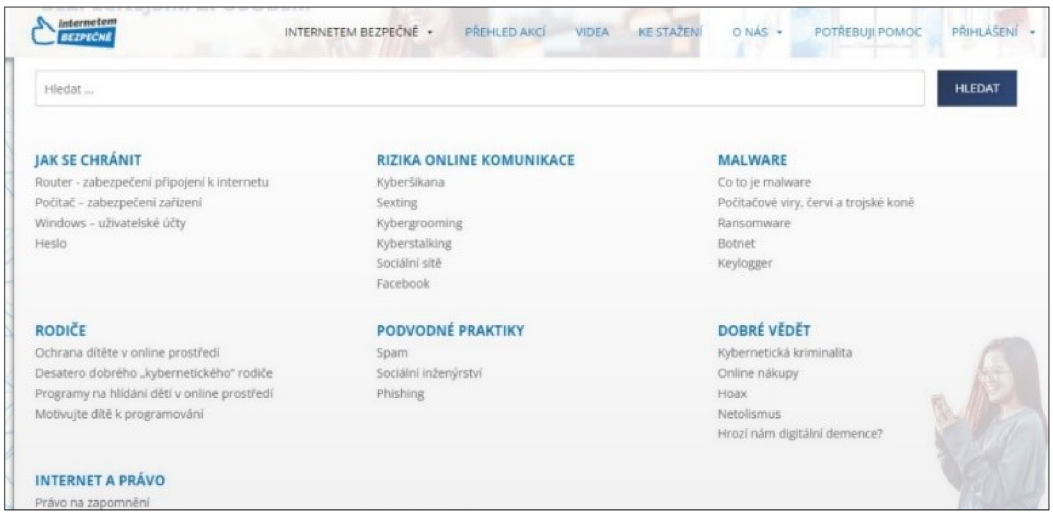
Kromě dobré legislativy a institucí, které zajišťuji bezpečnost eGovernmentu, je dalším pilířem osvěta a vzdělávání. Je potřeba neustále občany seznamovat s možnostmi elektronické komunikace ve veřejné správě. Vzdělávání probíhá jak uvnitř veřejné správy (vzdělávání úředníků), tak prostřednictvím různých vzdělávacích aktivit pro širokou veřejnost. Základem je však vzdělávací soustava a důraz na získání kompetencí v digitálním světě. Je třeba doplnit, že vzdělávání v bezpečném používání internetu snižuje také riziko kriminality na internetu. I když to je z určitého pohledu boj s větrnými mlýny. Vždy se najde někdo, kdo naletí

[47] BIS, dostupné z https://www.bis.cz/kyberneticka-bezpecnost/ [cit. 2022-03-16]
[48] UOOU, https://www.uoou.cz/ [cit. 2022-03-16]

podvodníkovi a nechá se bláhově obelstít. Může to být seznámení na internetu s atraktivním protějškem, který postupně vyláká z oběti nemalou částku. Může to být vidina bohatství a následování rad někoho, koho dobře neznáme. Rádoby výhodné a rychlé investice do čehokoliv prostřednictvím internetu.

Může to být také falešné vylákání přístupových údajů do internetového bankovnictví nebo k platebním kartám. Může to být kliknutí na odkaz v mailu, který útočníkovi umožní získat naše data na počítači nebo mobilu. A tak bychom mohli pokračovat. Možnosti kybernetického zločinu se rozvíjejí s novými technologickými možnostmi a dostupností on-line aplikací. Možnosti vzdělávání v oblasti "bezpečného internetu" zabrání velkým emocionálním i finančním ztrátám. Uvádím odkazy na zajímavé projekty neziskových organizací, policie ČR, nebo soukromých subjektů:

- https://www.e-bezpeci.cz/
- https://native.seznamzpravy.cz/jste-na-internetu-v-bezpeci/
- https://www.internetembezpecne.cz/
- https://www.policie.cz/clanek/kyberkriminalita.aspx



Obrázek 16. Projekt Internet bezpečně, dostupné z https://www.internetembezpecne.cz/ [cit. 2022-03-16]

O vzdělávání v digitální gramotnosti se stará také Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). „Naší primární cílovou skupinou pro vzdělávání jsou úředníci, zaměstnanci veřejné správy a další osoby podle Zákona o kybernetické bezpečnosti. Do sekundární skupiny řadíme žáky mateřských,

základních i středních škol, u kterých se snažíme přispívat k budování návyků bezpečného informačního chování. Na několika úrovních spolupracujeme s univerzitami, kterým poskytujeme přednášky a další součinnost při přípravě budoucích odborníků. Nezapomínáme ani na širší veřejnost, kde nabízíme rodičům oporu při jejich nelehkém úkolu – výchově dětí v digitální éře. Seniorům pomáháme orientovat se na internetu a využívat jeho výhod bez toho, aby se stali snadnou obětí podvodníků a útočníků.“[49]

[49] NUKIB, Vzdělávání, dostupné z https://www.nukib.cz/ [cit. 2022-03-16]

5. eGovernment v samosprávě

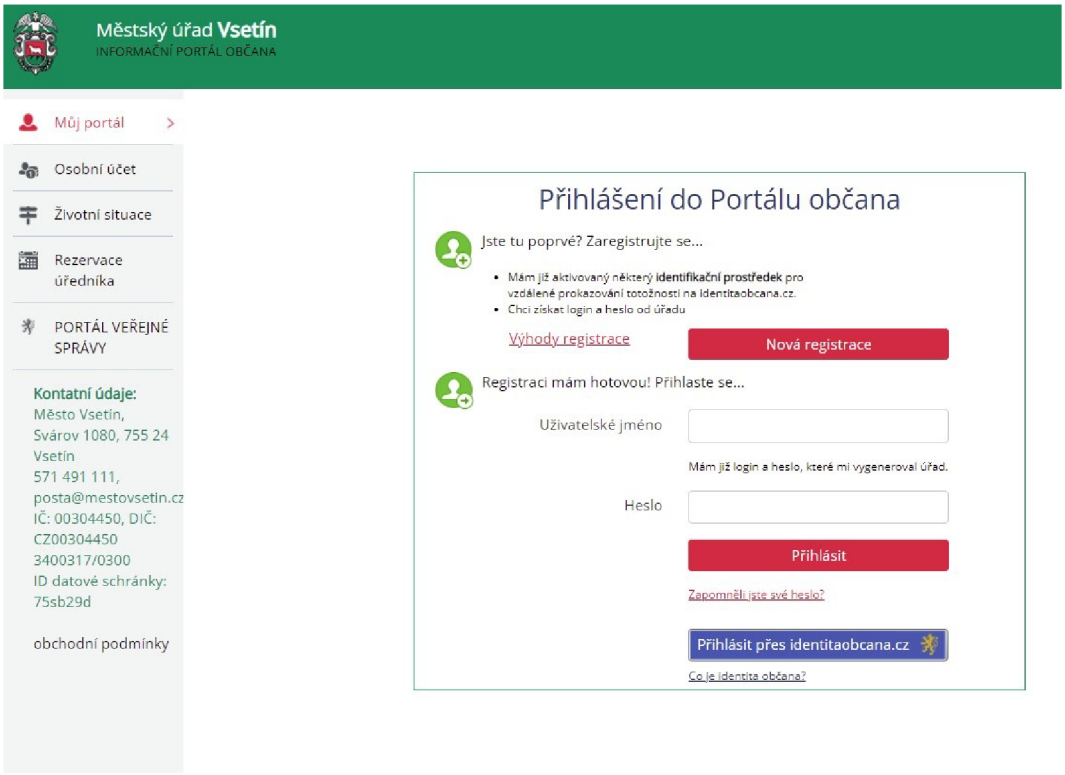
Správné fungování a rozvoj eGovernmentu je závislý na bezpečném fungování informačních systémů. Informační systémy veřejné správy zajišťuje především stát. Základní registry, datové schránky, elektronickou identitu a technickou infrastrukturu garantuje státní správa. Obce ve své samosprávné funkci využívají eGovernment jen v omezené míře. Na obce ale stát přenesl některé své úkoly, které obec zajišťuje pro stát. Obec tak vykonává funkci státní správy v přenesené působnosti.

„Národní projekty eGovernmentu státní správy vedou (nebo alespoň předpokládají) přizpůsobování IS obcí a krajů z oblasti samosprávy. V případě projektů českých samospráv se kromě jejich vazby na IS státní správy projevuje jejich větší samostatnost, která je limitována kapacitami jednotlivých obcí a krajů (a různých forem jejich spolupráce) a standardizačními nástroji stanovenými na národní úrovni. Mezi důležité standardizační nástroje patří v ČR např. požadavky zakotvené v zákoně o ISVS (včetně představených povinností spojených s dlouhodobým řízením IS), v zákoně o svobodném přístupu k informacím (jde např. o povinnost aktivně zpřístupňovat některé druhy informací na webových stránkách), v zákoně o e-podpisu či správním řádu. Mezi relativně nové povinnosti patří i povinnost obcí komunikovat s určitými typy subjektů prostřednictvím datových schránek a zabezpečit vlastní činností či ve spolupráci s jinými elektronickou spisovou službu.“[50]

Portál občana, zmiňovaný v 2. kapitole (Digitalizace služeb veřejné správy) kromě služeb státní správy integruje i digitální služby samospráv. Může se jednat o služby jako: úhrada místních poplatků přes platební bránu, funkce hlášení závad na interaktivní mapě, elektronická úřední deska nebo digitální formuláře pro řešení životních situací. Po přihlášení do Portálu občana si každý může na svém profilu přidávat „dlaždice“ úřadů, které slouží jako portál pro digitální služby úřadu. Stejným způsobem si můžeme přidat i „dlaždici“ konkrétní obce. Pokud v seznamu „Na úřad on-line“ není obec, kterou hledáme, může být nalezena ještě na „Seznamu

[50] ŠPAČEK, David. EGovernment: cíle, trendy a přístupy k jeho hodnocení. V Praze: C.H. Beck, 2012., s.93-94

poskytovatelů a služeb“ na www stránkách Identita občana (https://info.identitaobcana.cz/). Některé obce umožňují vstup do portálu svých služeb pouze na svých www stránkách. Možnost přihlášení je také prostřednictvím své elektronické identity.



Obrázek 17. Informační portál občana Vsetína, dostupné z https://portal.mestovsetin.cz/portal/mujportal.html [cit. 2022-03-16]

5.1. Správa eGovernmentu v malých obcích

Tato práce je zaměřena na malé obce, které jsou svojí velikostí sice bezvýznamné, ale z hlediska počtu nejrozšířenější. Jak již bylo uvedeno v 1. kapitole (Systém veřejné správy v ČR), malých obcí (do 1000 obyvatel) je v České republice 80 % z celkového počtu více jak 6 000 obcí. Malé obce mají specifický ráz a některé společné rysy. Zastupitelé těchto obcí jsou většině lidem v obci dobře známi. Při některých rozhodováních se tak berou v potaz i vztahy (ať už v dobrém nebo v horším smyslu). Při jednáních na obecním úřadě jsou lidé více osobní oproti větším sídlům. Obecní úřad malé obce se skládá mnohdy jen ze starosty a účetní obce, která vykonává další potřebné záležitosti obecního úřadu.

Vnější služby eGovernmentu v malé obci

Vzhledem k tomu, že eGovernment je řešen převážně na centrální úrovni, dostupnost služeb eGovernmentu je prakticky z každého místa s pokrytím internetu. Na úrovni státní správy jsou těmi vstupními dveřmi Portál veřejné správy. Obce mohou komunikovat elektronicky prostřednictvím svých www stránek. Jsou to takové virtuální dveře, které otvírají úřad 24 hodin denně. Prostřednictvím svých www stránek obce nejenom informují o aktuálním dění v obci. Zveřejňují na svých elektronických úředních deskách dokumenty podle správního řádu. Někde umožňují přístup k elektronickým formulářům. Lidé si je mohou vyplnit on-line nebo vytisknout (a vyplnit doma) a urychlit tak vyřizování úředních záležitostí. Někde mají obce na svých www stránkách možnost přihlásit se do osobního portálu občana (viz obrázek 17) a mít přehled například o svých místních poplatcích a zaplatit je bez návštěvy úřadu. Osobní portál občana uzpůsobený pro malé obce nabízí firma Gordic.[51]Je možné si vybrat mezi licencí s instalací na server obce nebo aplikaci provozovat v cloudu u dodavatele. Cena takového řešení podle telefonního dotazu u firmy Gordic začíná na 2000 Kč za měsíc.

Malé obce poskytují jen v omezené míře vnější služby v oblasti eGovernmentu. Samozřejmostí je komunikace s institucemi a fyzickými osobami prostřednictvím datových schránek (správa datových schránek je zajištěna na státní úrovni). Stále rozšířenější se stává elektronická komunikace prostřednictvím interaktivních aplikací. Aplikace Mobilní rozhlas nebo Hlášení rozhlasu.cz. umí rozesílat texty a přílohy na mailové a telefonní kontakty občanů. Občané se sami zaregistrují a mohou si vybrat oblast aktualit, které chtějí dostávat. Součástí těchto aplikací je i možnost zasílání různých podnětů od občanů, jako je např. poničený mobiliář, nesprávné značení apod. Další elektronickou službou obecních úřadů mohou být informace z oblasti ochrany obyvatelstva před nebezpečnými jevy, jako jsou přírodní hrozby nebo jiný druh nebezpečí. Prostřednictvím webových stránek lze informovat obyvatelstvo o výšce hladiny toků nebo jiných nebezpečných okolnostech. Například povodňový varovný informační systém obcí Hornolidečska umožňuje sledovat on-line vývoj výšky hladiny řek (Senice, Bečva) a vyhlašovat

[51] Osobní portál občana, dostupné z https://gordicportalobcana.cz/varianty/ [cit. 2022-03-16]

obecním rozhlasem případné pokyny v krizových stavech. Již zavedenou službou s více jak desetiletou tradicí je služba Czech POINT, která stála na začátku zavádění eGovernmentu v České republice. Služba Czech POINT umožňuje lidem, kteří ještě nemají zřízenou elektronickou identitu, komunikaci s úřady veřejné správy. Prostřednictvím Czech POINTu mohou lidé získat výpisy z různých rejstříků, katastru nemovitostí, nebo si založit datovou schránku. Czech POINT také umožňuje konverzi dokumentů z elektronické do listinné podoby a naopak. Další službou z oblasti elektronické komunikace úřadu může být např. elektronická vývěska, která se uplatní spíše u větších obecních úřadů.

Vnitřní procesy eGovernmentu v malé obci

Lokální informační systém obecního úřadu je v současné době (v době informačních technologií) nezbytný nástroj veřejné správy. Informační systém zahrnuje potřebný hardware (PC, server, síťové prvky), software (operační systém, elektronická spisová služba, webový prohlížeč apod.) a propojení do komunikační sítě. V tomto systému je zpravidla nastavena forma sdílení dokumentů, předávání dat a zálohování. Jelikož systém nemůže plně pracovat uzavřeně bez výměny informací s vnějším světem, musí být připojen k síti internetu a také zabezpečen proti neoprávněnému proniknutí do vnitřních databází. Součástí informačního systému malého obecního úřadu jsou především elektronická spisová služba a účetní software. Další možný software, který je využíván ke zpracování lokálních dat, je například evidence majetku, evidence obyvatel, evidence smluv, apod.

Páteří elektronizace obecního úřadu je elektronická spisová služba. Ta zajišťuje oběh elektronických dokumentů uvnitř úřadu. Odpovědný pracovník za spisovou službu třídí došlou poštu (elektronickou i papírovou) a přiděluje ostatním zaměstnancům obecního úřadu dokumenty podle jejich kompetencí. Tito pracovníci přidělené dokumenty vyřizují a zadají do systému datum, kdy byly dokumenty vyřízeny. Tímto procesem má každý dokument zapsanou historii a průběh zpracování. U dokumentu se při evidenci zadává také skartační znak, který udává, co se má s dokumentem stát po proběhnutí doby "použitelnosti" dokumentu (skartační lhůty). K vyznačení skartačního znaku se používají písmena A (archiv), S (skart) nebo V (výběr), za která se napíše číslice, udávající počet let skartační

lhůty. Skartační lhůta začíná běžet 1. lednem následujícího roku po vyřízení dokumentu nebo uzavření spisu. Například značka S3 znamená dát do skartu (stoupy) za tři roky, A5 znamená předat do archivu k trvalému uložení za pět let a značka V3 znamená po třech letech rozhodnout, zda dát do skartu nebo do archivu. A podobně jako se předávají dokumenty se skartačním znakem "A" do okresních archívů, předávají se elektronické dokumenty označené tímto znakem do Národního archívu. Po elektronickém předání a potvrzení se mohou ze spisovny smazat.

Správce sítě

Pokud má obec lokální počítačovou síť, zpravidla má někoho, kdo se stará o bezproblémový chod této sítě. Tento správce sítě by měl být přítomen při návrhu informačního systému a při konfiguraci a zapojení nových prvků do sítě. Měl by mít dokonalý přehled o zabezpečení jednotlivých prvků i celé lokální sítě proti vnějším i vnitřním hrozbám. Správce sítě by měl znát slabiny celého systému a komunikovat se starostou, jakou úroveň zabezpečení má lokální síť splňovat. Správce sítě by měl také zajistit spolehlivé a pravidelné zálohování všech relevantních dat v systému. Požadavky systému by měl stanovit starosta, technické parametry systému by měl řešit správce sítě.

Administrátor orgánu veřejné moci

Institut administrátor orgánu veřejné moci (OVM) byl zaveden s povinností obcí zřídit si datovou schránku podle zákona[52] z roku 2008. Administrátor OVM by neměl být volený zastupitel. Měl by to být zaměstnanec obecního úřadu nebo spolehlivá externí fyzická osoba. Administrátor OVM totiž zpřístupňuje elektronické agendy jednotlivým uživatelům obecního úřadu. Jedná se o centralizované informační systémy jako: informační systém základních registrů a přístup do Czech POINTu. Administrátor zaregistruje do portálu "Czech point/správa dat" vydané přístupové certifikáty nebo elektronické podpisy jednotlivých osob obecního úřadu. Kromě přístupů do centrálních informačních systémů přiděluje jednotlivým uživatelů obecního úřadu tzv. agendové činnostní

[52] Zákon 300/2008 Sb., dostupné z https://www.zakonyprolidi.cz/cs/2008-300 [cit. 2022-03-16]

role. Bez tohoto přidělení by uživatel neměl přístup do agendy, kterou má vykonávat. Jak je vidět, administrátor OVM musí být vysoce spolehlivá osoba, na které závisí důvěryhodnost a bezpečnost dostupných dat v informačních systémech veřejné správy.

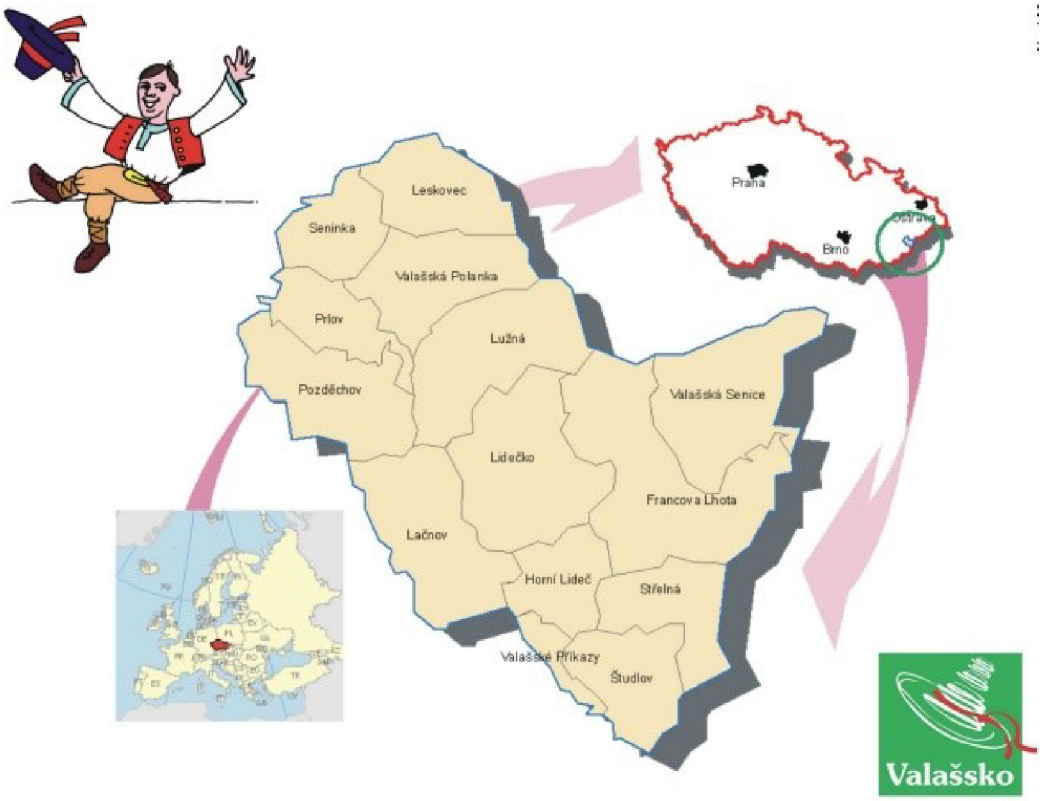
Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je nejmladší funkce spojená s elektronizací obecního úřadu. Funkci pověřence definuje Zákon o ochraně osobních údajů. Pověřenec je "styčným důstojníkem" mezi zpracovatelem osobních údajů (obcí) a osobami, kterých se zpracování týká (občané). V případě bezpečnostních incidentů (ztráta databází týkající se osobních údajů) komunikuje s Úřadem pro ochranu osobních údajů (ÚOOÚ). Provádí poradenství správci či zpracovateli osobních údajů včetně zaměstnanců. Navrhuje opatření k zabezpečení osobních dat a hlídá soulad zpracování osobních údajů (v informačním systému obce) s aktuální legislativou.

5.2. Stav eGovernmentu v obcích na Hornolidečsku

Mikroregion Hornolidečsko zahrnuje území 15 obcí - Francova Lhota, Horní Lideč, Lačnov, Lidečko, Střelná, Študlov, Valašská Senice, Valašské Příkazy, Valašská Polanka, Lužná, Prlov, Pozděchov, Leskovec, Seninka, Ústí.[53] Je součástí Zlínského kraje v okrese Vsetín a leží u státních hranic se Slovenskou republikou. Patří tak mezi tzv. "příhraniční mikroregiony". Část území mikroregionu se nachází v Chráněné krajinné oblasti Beskydy a částečně také CHKO Bílé Karpaty. Patří mezi nejhornatější a nejlesnatější území v celé České republice. Jedná se o typický venkovský mikroregion s 12,2 tis. obyvateli a rozlohou 170,1 km^2. Pro jednotlivé obce jsou typická dlouhá a úzká údolí se značně svažitými pozemky. Území vymezená katastry jednotlivých členských obcí jsou snadno přístupná železnicí spojující Moravu se Slovenskem nebo silnicí I/57 ve směru Vsetín - Púchov.

[53] Hornolidečsko, dostupné z http://www.hornolidecsko.cz/cz/1-clenske-obce.html [cit. 2022-03-16]



Obrázek 18. Mapa Sdružení obcí Hornolidečska, dostupné z http://www.mashornolidecska.cz/files/files/SPL/SPL_MASH_2007-13_final.pdf [cit. 2022-03-16]

Dotazníkové šetření

Dotazník mapující stav eGovernmentu na Hornolidečsku byl vytvořen v aplikaci Google Formuláře a rozeslán na mailové adresy všech starostů obcí Hornolidečska. Na dotazník odpovědělo 12 starostů z 15 oslovených obcí, což je 80 % oslovených. Dotazník měl krátký popisek a 20 otázek. Otázky mapovaly stav elektronizace na obecních úřadech. Jaké digitální nástroje obec využívá, jak funguje lokální počítačová síť, jak jsou zabezpečená data a jaké jsou náklady na údržbu celého systému.

Dotazník zahrnoval tyto otázky:

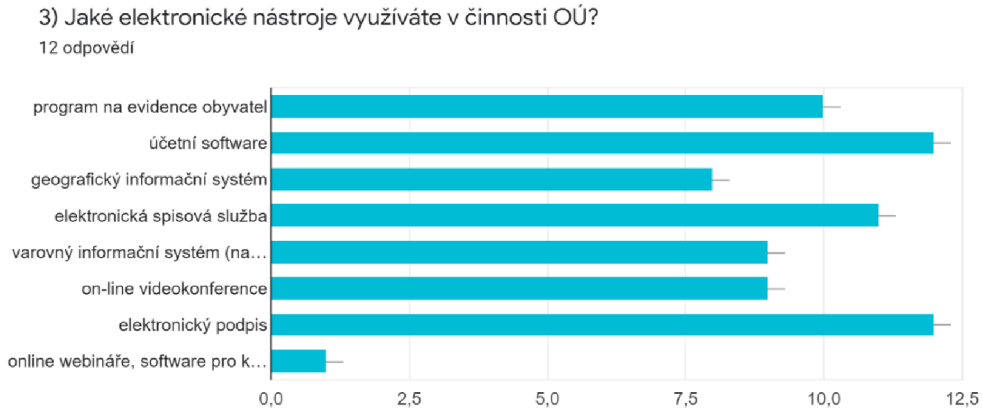
1) Název obce.
2) Počet obyvatel.
3) Jaké elektronické nástroje (evidence obyvatel, účetní SW, aj.) využíváte v činnosti OÚ?

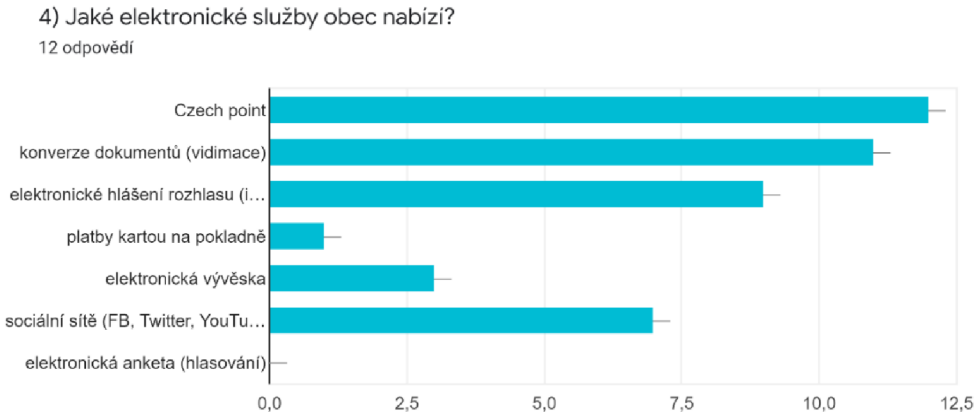
4) Jaké elektronické služby obec nabízí (Czech POINT, konverze dokumentů, platby kartou na pokladně, elektronická vývěska, elektronické formuláře na www aj.)?
5) Má obec pověřence pro ochranu osobních údajů (zaměstnanec, externí)?
6) Má obec správce PC sítě (zaměstnanec, externí)?
7) Má obec lokálního administrátora pro Czech POINT (zaměstnanec, externí)?
8) Jaké jsou celkové roční náklady na pověřence, administrátora a správce?
9) Jaké jsou celkové roční náklad na softwarové vybavení (evidence obyvatel, účetní SW, aj.)?
10) Jaké jsou celkové roční náklad na hardware (nákupy za deset let/10)?
11) Jakým způsobem jsou propojeny počítače v rámci OÚ?
12) Jakým způsobem se zálohují data?
13) Jak často probíhá záloha dat?
14) Jak často probíhá školení obsluhy PC na bezpečné zacházení s uloženými daty?
15) Máte záložní zdroj elektrické energie?
16) Jaký druh připojení do internetu má OÚ (ADSL, WiFi, optický kabel, jiný)?
17) Jakým způsobem je ochráněna vnitřní PC síť (firewall, antivir, routek, jiné….)?
18) Jakým způsobem je zabezpečena vnitřní WiFi síť (pokud je, jak)?
19) Jak vám elektronizace pomáhá v práci úřadu (zpomaluje práci, neutrálně, pomáhá v práci)?
20) Jak dlouho jste ve funkci starosty?

Odpovědi a vyhodnocení je v grafech a tabulkách níže. Obce, které odpověděly v šetření (v závorce počet obyvatel):

- Valašská Polanka (1440)
- Střelná (574)
- Leskovec (650)
- Francova Lhota (1500)
- Valašská Senice (421)
- Horní Lideč (1370)
- Prlov (525)
- Seninka (312)
- Valašské Příkazy (310)
- Lužná (618)
- Obec Ústí (620)
- Pozděchov (585)

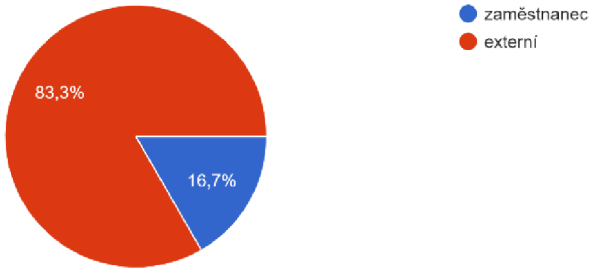
eGovernment je někdy charakterizován jako elektronizace veřejné správy. Dá se říct, že většina agend obecních úřadů se již přesunula z papírové evidence na elektronickou. Téměř každá obec pracuje s elektronickou spisovou službou, Czech POINTem, datovou schránkou nebo základními registry.



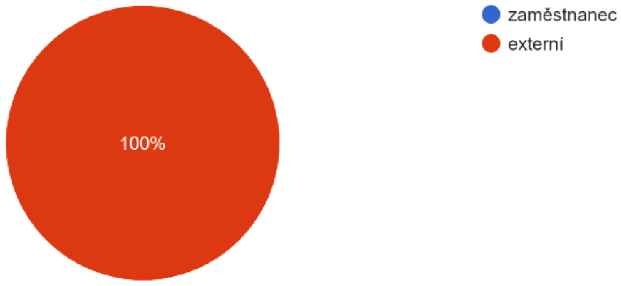


Dále se dotazník zaměřil na správu eGovernmentu na obecním úřadě. Kdo se stará o údržbu systému? Jak je zajištěna správa sítě, správa přístupů a ochrana osobních údajů? Pověřenec pro ochranu osobních údajů i správce PC sítě a lokální administrátor je zajišťován převážně externě. Pouze v menší míře je pověřenec a lokální administrátor zajišťován z řad zaměstnanců obecního úřadu. Z toho vyplývá i celková výše nákladů na zabezpečení eGovernantu v malých obcích.

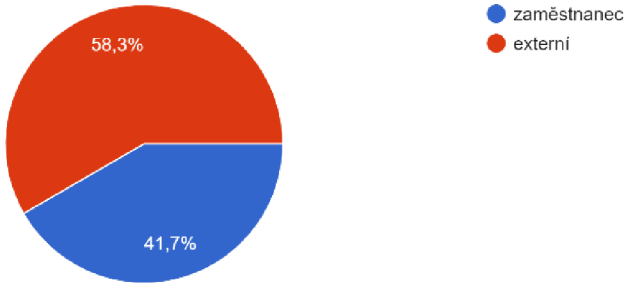
5) Má obec pověřence pro ochranu osobních údajů?
12 odpovědí



6) Má obec správce PC sítě?
12 odpovědí

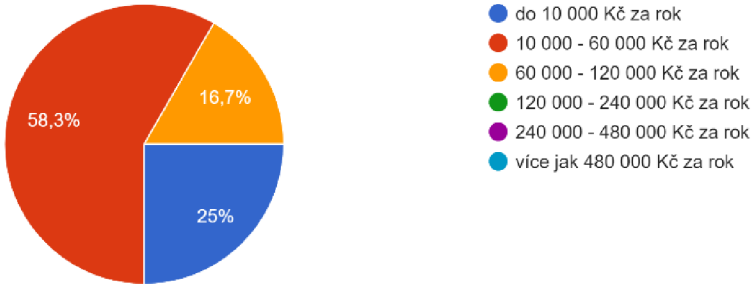


7) Má obec lokálního administrátora?
12 odpovědí

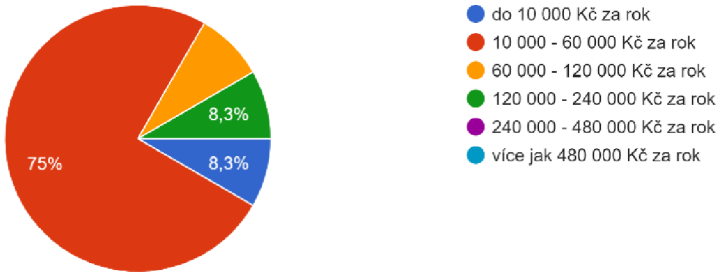


Celkové náklady na obsluhu informačního systému (správce sítě, lokální administrátor, pověřenec pro ochranu osobních údajů) na malé obci se pohybují nejčastěji v intervalu 10 000 – 60 000 Kč za rok. Stejný interval byl nejčastěji uváděn v dotazníku u ročních nákladů na software a hardware.

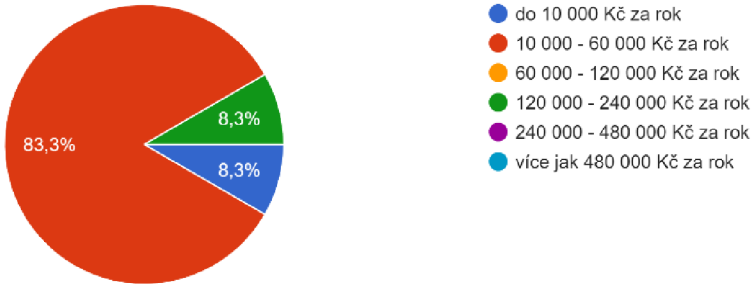
8) Jaké jsou celkové roční náklady na pověřence, správce a administrátora (celkem)?
12 odpovědí



9) Jaké jsou celkové roční náklady na softwarové vybavení OÚ (nákup a údržba SW)?
12 odpovědí



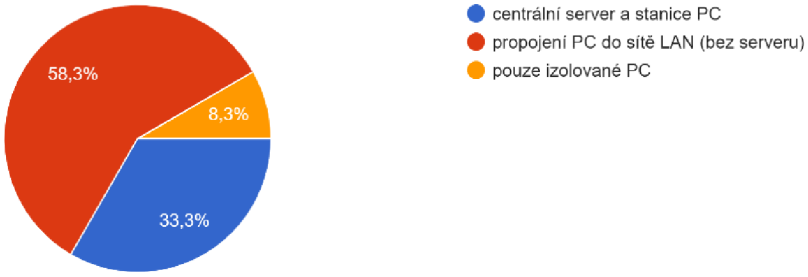
10) Jaké jsou celkové roční náklady na hardware (nákupy za deset let/10)?
12 odpovědí



Další otázky z dotazníku byly zacílené na informační systém obecního úřadu a zabezpečení dat v systému. Nejčastěji jsou pracovní stanice na obecním úřadě zapojené v síti LAN. Zálohování dat probíhá nejčastěji denně nebo měsíčně.

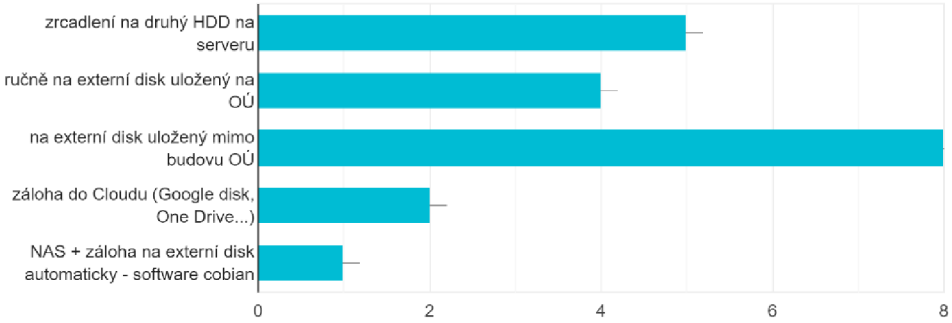
11) Jakým způsobem jsou propojeny počítače v rámci OÚ?

12 odpovědí



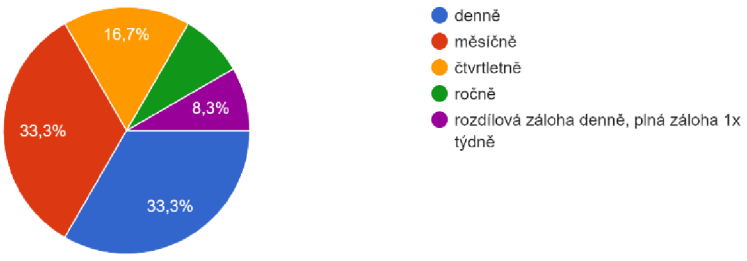
12) Jakým způsobem se zálohují data?

12 odpovědí



13) Jak často probíhá záloha dat? (Kdyby se poškodil server/ datový PC, jak starou zálohu byste mohli obnovit?)

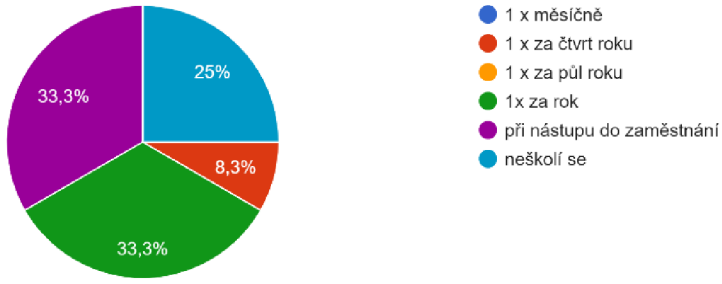
12 odpovědí



Po odpovědích na zabezpečení dat v systému, byly otázky zacílené na školení obsluhy a zajištění celého systému v případě výpadku elektrické energie. Na způsob připojení informačního systému do internetu odpověděla většina starostů tak, že mají bezdrátové připojení, třetina využívá ADSL připojení a nejméně obecních úřadů je napojeno na optický kabel.

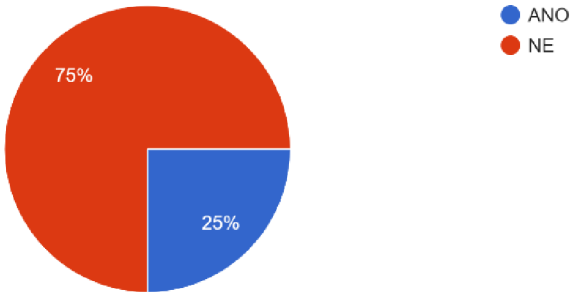
14) Jak často probíhá školení obsluhy PC na bezpečné zacházení s uloženými daty?

12 odpovědí



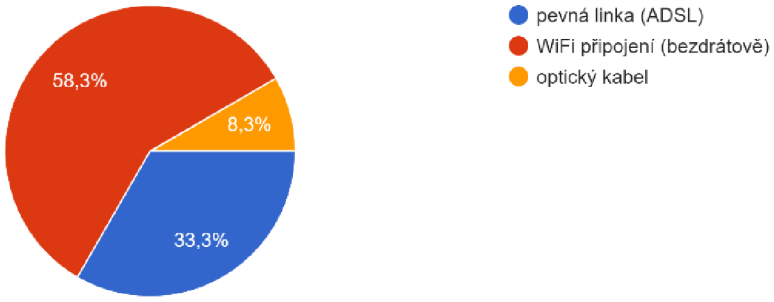
15) Máte záložní zdroj elektrické energie pro OÚ?

12 odpovědí



16) Jaký druh připojení do internetu má OÚ?

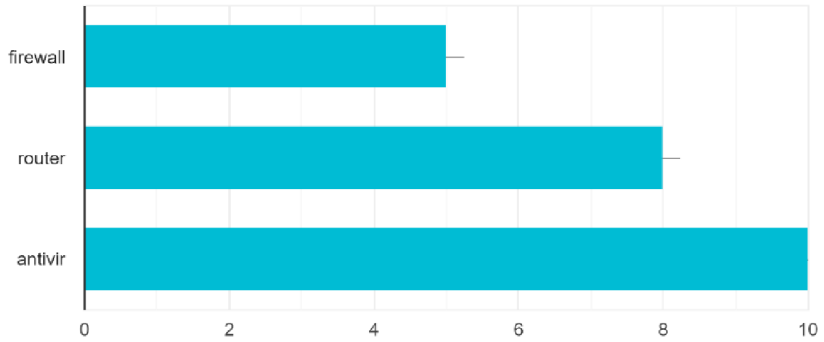
12 odpovědí



Bezpečnost vnitřní informační sítě mapují další otázky. Jaké jsou použity ochranné prvky v systému? Jak je zabezpečená vnitřní WiFi síť?

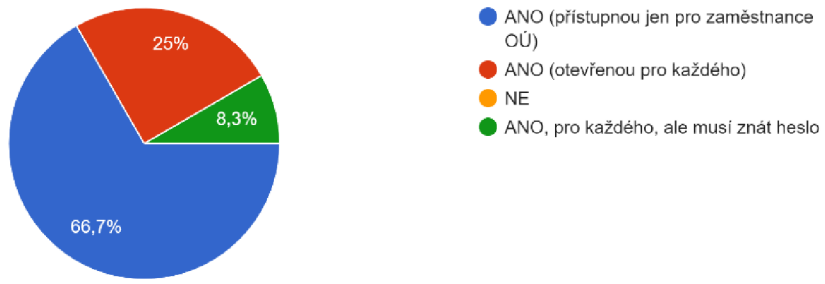
17) Jakým způsobem je ochráněna vnitřní PC síť?

12 odpovědí



18) Má OÚ vnitřní WiFi síť?

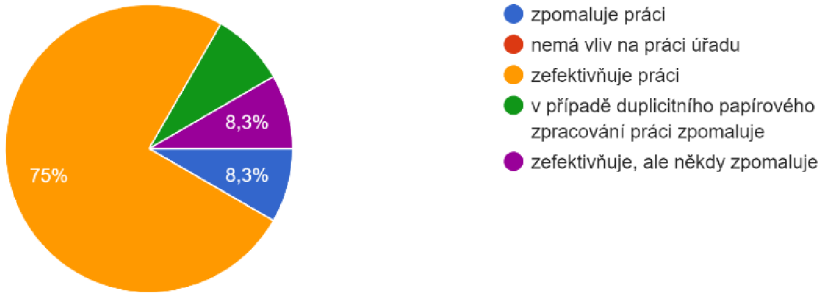
12 odpovědí



Předposlední otázka a odpovědi vyjadřují subjektivní postoj a zkušenosti s elektronizací obecního úřadu. Poslední otázka zobrazuje délku působení starostů v úřadě. Většina starostů odpověděla, že jsou v prvním volebním období. Čtvrtina je ve funkci více jak 4 roky a třetina odpověděla, že jsou ve funkci více jak 12 let.

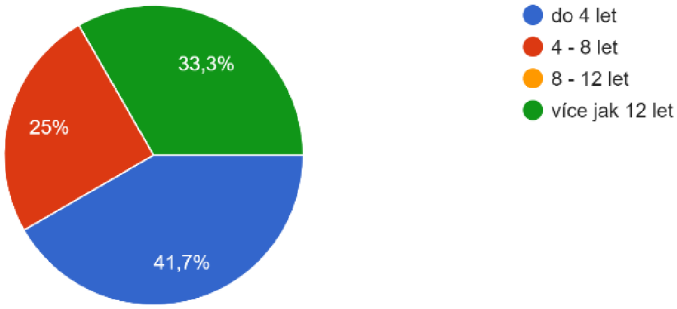
19) Jak vám elektronizace pomáhá v práci úřadu?

12 odpovědí



20) Jak dlouho jste ve funkci starosty

12 odpovědí



Strukturovaný rozhovor se starosty obcí

Z celkově 15 oslovených starostů, zareagovalo osm, což je více jak polovina. S těmito osmi statečnými jsem si domluvil schůzku a udělal rozhovor na základě předem daných otázek. Rozhovor jsem zaznamenával rovnou do textu (prostřednictvím aplikace Speech to text na mobilním telefonu). Text jsem následně musel opravit, protože převod z mluveného slova do textu byl v některých slovech zkomolený. Nicméně výsledný text po drobné korekci odpovídá záznamu. Strukturovaný rozhovor vyjadřuje názory jednotlivých starostů na eGovernment. Rozhovor jsem vedl podle následujících otázek:

1) Co Vás napadne v souvislosti se slovem eGovernment?
2) Do jaké míry se zajímáte o vývoj nových technologií v oblasti ICT?
3) Setkal jste se v minulosti se zavirovaným PC nebo ztrátou dat v rámci úřadu?
4) Máte za to, že OÚ je dostatečně chráněn proti ztrátě dat?
5) Máte přehled o tom, jak jsou zabezpečeny PC a jejich přístup do internetu?
6) Jaká rizika vnímáte s nástupem elektronizace obecních úřadů?
7) Jak vám může zavádění eGovernmentu ulehčit práci starosty?

A jaké názory starostové vyjadřovali? Níže jsou zaznamenány odpovědi v autentické podobě, bez jazykových úprav. Jsou tu vybrány pouze některé odpovědi (v původní podobě), aby dokreslily situaci a vývoj elektronizace na obecních úřadech malých obcí. Je třeba říct, že starostové odpovídali bez přípravy a proto odpověď může být někdy "kostrbatá". Při každém rozhovoru jsem zdůraznil, že nejde o "správné odpovědi", ale o skutečné názory starostů na postup elektronizace na obecních úřadech.

Co tedy vidí starostové za pojmem eGovernment?

Starosta z Valašské Polanky:

„Já si to představuji tak, že bude vytvořený takový systém v naší republice, že když se člověk narodí, zavede se mu rodný list. Tam budeš mít nějaké číselné údaje o tom, že jsi nějaký František Vopršálek a že patříš rodičům těm a těm. V podstatě ten systém bude fungovat tak, že když budeš dítě, tak rodičům půjdou automaticky podle jejich výdělku nějaké příspěvky na dítě, anebo máš nárok na to, že dostaneš příspěvek na bydlení podle příjmu rodičů. Že se to začne prostě v tom počítačovém systému podle nastavených pravidel všecko počítat tak, že se o tobě ví, že jsi student, že odejdeš od rodiny, že už máš samostatnou domácnost… A že někdo někde spočítá, kolik vydělá ten nebo onen a v jaké výši odvede nějakou daň. Daň odvede do jednoho místa jako jednu částku a že se o to prostě všechny ty ostatní instituce podělí. A že když nahlásím, že jsem bez práce, tak prostě a jednoduše automaticky ten systém se přepne do pozice, že jsi bez práce a že ti začne chodit nějaká dávka, na kterou máš nárok. A že to je někde spočítané a jednoduše to skončí

celé tím, že zase začneš chodit do práce. Tak to půjde, než v podstatě umřeš. Tak se nahlásí úmrtní list. A vlastně celý ten systém končí beztoho, aniž bys kdy navštívil jakýkoliv úřad a musel vyplňovat vstupní formulář. A jak debil si furt pamatovat rodné číslo, číslo občanského průkazu, a dívat se na každého otráveného úředníka státní správy potažmo samosprávy. A v podstatě tak to zjednoduší práci. To si představuji pod pojmem eGovernment."

Starosta z Lidečka:

„Myslím si, že už v dnešní době elektronizace představuje zjednodušení pro občany a zároveň potom možnost pro obce nějaké věci rychleji a lépe vyřídit. Některé řízení, si myslím, že to úplně nezrychlí, protože někdy zrychlí naopak ten osobní kontakt na místě. Takových těch papírových věcí, které jsou takové jako v podstatě jenom pro papír, tak určitě to smysl má. A digitalizace v tomto směru pomáhá. Je pravdou, že starší generace s tím má určité problémy, ale už ta střední a mladší, to se ani nebavím, tak pro ni je to skoro jako samozřejmost. A je to vidět na všech frontách. Takže určitě to hlavně mladším a střední generaci pomůže zrychlit některé formální obecné věci, například u některých náročnějších stavebních řízeních. Ve finále někdy je důležité zase se úplně oprostit od osobního kontaktu, protože úředníci jsou zavalený."

Starosta z Francovy Lhoty:

„U nás se o nové technologie zajímá místostarosta. Má to výhodu v tom, že ho to strašně baví. Zavedli jsme například elektronické knihy jízd. On si vypracoval svůj program, nakoupili jsme do každého auta jednoduchou aparaturu. Máme přehled o všech aut, o jejich provozu."

Co se týká zabezpečení obecního úřadu a jeho informačního systému starostové soudí toto:

Starosta z Valašské Polanky:

„Počítače jsou zabezpečeny tak, že je prostě máme zaheslované, že do každého počítače se dostane člověk jenom přes svoje heslo. No a přístup k internetu, přístup k internetu máme volný, tam neumím říct, jaký by měl být. Já když potřebuji přístup

na internet, tak si tam pěkně kliknu na ikonku a jsem tam, ale jak bych to měl nějak chránit, to mě nikdo neřekl. Jako jo, samozřejmě vím, že navštěvovat pochybné stránky je asi rizikové, takže to zařídím jakýmsi interním pokynem. Že bych to nějak speciálně kontroloval, to ale nedělám.

Starosta z Lidečka:

„Tak to si myslím, že úplně asi zabezpečit stoprocentně nejde. My v současné době máme tady alarm, máme tady kamerový systém, to znamená nějaké základní zabezpečení, samozřejmě zámky a ostatní věci. Ano, samozřejmě jsou věci, které nás dotlačil GDPR. Máme pověřence, spolupracujeme se sdružením samospráv, kde přispíváme měsíční částku na to, že se vlastně o to starají. Informují nás, nějakým způsobem máme základní povědomí o tom, co dělat. Máme tady externí harddisk a máme vlastně hromadné úložiště, takže se něco zálohuje. A pak se některé data ještě posílá úplně mimo budovu, na nějaké úložiště. To je takový ten základ. Jak je zabezpečený přístup do internetu? Přiznám se, že úplně nevím, spíš spoléháme na toho providera, který v podstatě to tady řeší. Máme vlastně teď Ústí.net s.r.o. Spoléháme v podstatě na něj, že co se týká tady tohoto, tak to má nějakým způsobem zabezpečené. Jaká rizika vnímáte s nástupem elektronizace obecního úřadu? Samozřejmě otázka je, do jaké míry ten personál, který na těch obecních úřadech je, jestli je schopen všechnu tu agendu posunout, aby všechno šlo vyřizovat elektronicky. Jestli nebudu muset posílit další lidi. Protože samozřejmě se jedná o určitou práci. Máme účetní, máme tady další spolupracovnici, tak si myslím, že toho mají nad hlavu. Je pravdou, že jsou využívání na to, co dřív třeba nebylo, jako třeba výpisy z katastru a ostatních věci, co slouží občanům. Takové jako spisová služba a tak dál, to už nějakým způsobem je vychytané. To si myslím, že se to pomaličku vychytává, spíše otázka toho, jestli by to nepřibývalo, kdyby měli být nápomocni v komunikaci státu a občanů, tak jestli jsme schopni třeba v tom personálním obsazení, které tu máme, to zvládnout, to nedokážu úplně říct. Toho výkonu státní správy tolik nemáme, ale samozřejmě jsou úřady, kde je výkon státní správy daleko větší. Co jsou ty pověřené úřady nebo obce s rozšířenou působností. Kde samozřejmě už na to mají personál. Takže myslím si, že tam se to nějakým způsobem už třeba jako umí a jsou daleko lépe vyškolení než třeba my, když to dělám jako kdyby okrajově.“

Starosta z Ústí

„Nevím, jestli je úřad dostatečně chráněn. Děláme ale maximum pro to, aby tomu tak bylo. Hackeři jsou asi o krok napřed před uživateli. O bezpečnost počítačové sítě se stará u nás správce počítačové sítě. Snažíme se hrozby vychytat. Doufám, že děláme maximum. Úplně ale nejde zabránit riziku ztráty dat."

Jak vnímají starostové rizika eGovernmentu v budoucnu?

Starosta z Valašské Polanky:

No, rizika vnímám s nástupem elektronizace obecních úřadů, že jak vypnou elektriku, tak se neudělá vůbec nic. To si myslím, že si uvědomuje každý. Já už jsem se zabýval myšlenkou, kterou jsem ale nedotáhl do konce, že asi uděláme náhradní zdroj nebo aspoň přípravu pro zapojení náhradního zdroje pro obecní úřad jako takový, protože kdyby neměla jít elektrika, tak nejde tím pádem ani počítač. A tím pádem vlastně nic nejsem schopen udělat. Chystáme se postavit nebo spravit budovu u kostela pro nový obecní úřad. A tam si myslím, že by mělo být součástí projektu nějaká ta instalace solárních panelů k nabití baterií, které by umožnily, aby ten úřad třeba den nebo dva z těch baterek jel. Takže uvidíme, co projektanti vymyslí, ale každopádně chceme mít tento problém aspoň takto vyřešený, že na pár dní bychom byli zajištění."

Starosta z Ústí:

„Pokud dojde asi k nějakému zneužití dat. Nebo možná někteří lidé nebudou umět komunikovat elektronicky. Může dojít k tomu, že nebudou rozumět elektronickým formulářům, že třeba bude pro ně lépe přehledný tištěný formulář, který mohou dostat přímo na úřadě."

Starosta z Valašské Senice:

„Jsem tu už 23 let, ale nesetkal jsem se ještě, že bychom měli počítač narušený nějakým virem nebo že by došlo ke ztrátě dat v rámci obecního úřadu, což je dobře. Přesto všechno zálohujeme. Teď budeme zřizovat elektronickou spisovku, abychom vyhověli zákonu."

Starosta z Leskovce:

„Jsou mezi námi lidé, kteří prostě těmi technologiemi nevládnou, kteří to prostě neumí použít. Sami mají problém mít dotykový telefon, takže používají furt starý tlačítkový a podobně.“

Starostka ze Študlova:

„Za jedno z rizik považuji neustále se zvyšující administrativu. Doufali jsme, že s nástupem elektronizace bude vše jednodušší, ale není tomu tak. Povinnosti narůstají jak s elektronickou spisovou službou, s archivnictvím, dále narůstají náklady na zajištění chodu celé elektronické administrace. Považuji za důležité zmínit křehkost celého systému při delším výpadku elektrické energie a nedostupnost těchto technologií pro starší a sociálně slabé lidi, kteří budou prakticky vyřazeni z možnosti využívat tyto technologie.

Jak eGovernment pomáhá starostům v malých obcích?

Starosta z Valašské Polanky:

„Jak eGovernment může pomoct starostovi? No, tak samozřejmě přímo asi ne, protože to je práce s lidmi, to není o počítačích. Takže jak jsem mluvil o tom, že bude všecko dohledatelné o každém člověku, který by se neměl bát, že někdo zneužil údaje. Tak tím, že to bude fungovat. Tak z toho bude mít samozřejmě užitek ten úředník samosprávy, ale starostovi si myslím, že to moc nepomůže.“

Starosta z Lidečka:

„Jestli mně to ulehčí práci starosty? Tak samozřejmě, já se na to dívám jako ze dvou pohledů. Digitalizaci nebo využití IT se nevyhneme. Myslím si, že ten trend je jasně nastavený a vlastně bude se to ještě rozšiřovat do dalších oblastí. Já za sebe si myslím, že by to neměl být problém, ulehčí to práci. Mluví se hodně o smart řešeních. Ale spíš se jedná o to, že každá obec, každý starosta by potřeboval vědět o řešeních, které někdo nějak zajímavě vyřešil. Když už nějaký problém nastane, tak často to bývá tak, že určitě to neřeší jenom sám, ale že těch lidí, co to řeší, je daleko víc. Takže taková ta databáze takových těch obecných problémů. Nebo nějakým způsobem poradit s konkrétním problémem. Například pálení trávy a takové ty věci, které vlastně potřebujeme vědět v souladu se zákonem, abychom se

nedostali do problémů. Takže jako určitě si myslím, že k ulehčení je tady potenciál, ale není to všelék.“

Starosta s Francovy Lhoty:

„Jak mi to pomáhá v práci? Tak já si myslím, že to víceméně určitě ulehčuje práci, nemusím tisknout tolik různých dokladů, a na druhé straně vám to taky něco přináší. Jako že se to musíte učit, …nové věci. Třeba spisová služba, naučit se to mi trvalo chvilku, ale teď už s tím vycházím. Je třeba na tom neustále pracovat. Zaprvé jsou nějaké modernizace nebo aktualizace, zadruhé člověk se s tím učí na základě nějakého školení. Je to záležitost praxe.“

Starostka ze Seninky:

„Pamatuji si zavádění počítačů, kdy to velmi urychlilo a usnadnilo práci. Určitě, pokud člověk umí s těmi programy pracovat, tak určitě to usnadňuje, ale má to svoje rizika. No, a musí se tam ty údaje zadávat. Pokud tady máme obsazení v počtu dva lidi, tak ze začátku by to přidělalo práci, potom asi by to práci ulehčilo. Myslím si, že zatím pořád ještě není všechno na takové úrovni, aby se zrušila listinná podoba, pokud se hledá něco staršího, tak asi pořád je lepší, když je tady něco založeno na papíře.“

6. Zabezpečení eGovernmentu v samosprávě

Ve 4. kapitole (Zabezpečení eGovernmentu ve státní správě) byly popsány nástroje ke snížení hrozeb na celostátní úrovni eGovernmentu. Důležité nástroje jako legislativa, technické a institucionální zabezpečení, vzdělávací systém mají ale dopad i na nižší úrovně eGovernmentu. Jedná se o vnější prostředí lokálního eGovernmentu. Následující kapitola se zaměří na vnitřní prostředí lokálního eGovernment. Je to oblast, kterou obce mohou bezprostředně ovlivňovat.

6.1. Řízení rizik informačního systému obce

Informační systém obecního úřadu musí být ochráněn před možnými hrozbami. Jak už bylo zmíněno ve 3. kapitole (Rizika eGovernmentu ve státní správě), můžeme si rozdělit hrozby na vnější a vnitřní hrozby. Vnější hrozbou mohou být například kybernetický útok. Na straně vnitřních hrozeb většinou stojí lidský faktor uvnitř organizace. Uživatelé na obecním úřadě proto musí být vyškoleni v zásadách bezpečné práce na internetu. Další důležitou součástí bezpečnosti je ochrana dat a to pravidelným zálohováním.

Součástí úvah o zabezpečení informačního systému zahrnuje stanovení toho, co je v systému nejcennější, co budeme chránit, co je tím aktivem. Obecně **aktivum** je všechno, co má pro subjekt hodnotu (která může být zmenšena působením hrozby). Aktiva se dělí na hmotná (například nemovitosti, cenné papíry, peníze apod.) a na nehmotná (například informace, předměty průmyslového a autorského práva, morálka a kvalifikace zaměstnanců, dobré jméno organizace apod.). [54] Z hlediska hodnot jsou nejdůležitější v eGovernmentu data. Proto podléhají zvláštní ochraně. V podmínkách malých obcí se zabezpečení dat odvíjí od bezpečnosti informačního systému obce. Obecně lze říci, že data musíme chránit před zneužitím (krádež dat) a také před znehodnocením (ztrátou dat).

[54] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8. (s.294)

Míru slabých míst aktiv vyjadřuje její zranitelnost. Aktiva chráníme před hrozbami, které ji ohrožují. **Hrozba** je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na aktiva nebo může způsobit škodu, resp. poškodit organizaci jako celek. Hrozby mohou byt přírodního nebo lidského původu a také náhodné nebo úmyslné. Mohou pocházet zevnitř i zvenčí organizace. Hrozbou může být například požár, přírodní katastrofa, krádež zařízeni, získáni přístupu k informacím neoprávněnou osobou, chyba obsluhy, apod. Pravděpodobnost ohrožení aktiv vyjadřuje riziko. „**Riziko** vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody (nežádoucímu následku).“[55] Hrozbám se snažíme vyhnout, pokud provádíme aktivní opatření. Smejkal (2010) definuje **Opatření** jako postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci). Snížení zranitelnosti nebo dopadu hrozby znamená snížení rizika. Opatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody. Taková opatření chrání aktiva dané organizace.

6.2. Bezpečností audit informačního systému obce

Než přistoupíme k zabezpečení informační sítě, musíme vědět, v jaké situaci se nacházíme a co můžeme očekávat. Bezpečnostní audit má odhalit slabá místa informačního systému. Bezpečnostní audit se může vztahovat na tyto oblasti:

- Fyzická bezpečnost – to se vztahuje na všechny prostory, kde jsou jednotlivé prvky technické infrastruktury informačního systému úřadu. Může se jednat o kanceláře, serverovou nebo technickou místnost.
- Technická infrastruktura – zahrnuje všechny počítače, síťové prvky (umožňují např. propojení počítačů), server, router (odděluje počítačové sítě) a napojení do veřejné sítě internetu.
- Používaný aplikační software – jsou všechny programy, které se využívají v rámci úřadu.
- Poučená obsluha – pracuje se svým počítačem a využívá přidělené aplikace.

[55] SMEJKAL, V. REIS, K. *Řízení rizik ve firmách a jiných organizacích.* Praha: GRADA Publishing, a.s., 3. rozšířené a aktualizované vydání, 2010. 488 s. ISBN: 978-80-247-3051-4, s.99

Aktivum v našem případě budou data (elektronické informace), která jsou využívaná v rámci úřadu. A zopakujme ještě krátce pojmy. Na chráněná data působí různé hrozby (přírodního nebo lidského původu). Hrozby mohou mít charakter požáru, krádeže zařízení, chyby obsluhy, úmyslného poškození, kybernetického útoku, ztráty dat. K prevenci vzniku škody provádíme opatření, která vedou například k lepšímu zabezpečení před kyberútoky, lepšímu fyzickému zajištění technické místnosti, pořízení fotovoltaické elektrárny jako záložního zdroje elektrické energie aj. Provedením bezpečnostního auditu dostaneme obrázek toho, v jakém stavu se informační systém úřadu nachází a jaké jsou jeho slabá místa.

Součástí bezpečnostního auditu může být i SWOT analýza. Ta kromě rizik a slabých míst ukazuje i na silné stránky organizace. Příklad takové SWOT analýzy, analýzy silných a slabých míst, příležitostí a hrozeb, ukazuje tabulka níže. Silné a slabé stránky vycházejí z analýzy současného stavu. Příležitosti a hrozby ukazují směr do budoucnosti. Hrozby ohrožují slabá místa naší organizace. Příležitosti znamenají použití silných stránek pro zamezení hrozeb v budoucnosti.

Silné stránky	**Slabé stránky**
Zaměstnanec OÚ má znalosti ICT	Nedostatek financí na bezpečnost
Vysoká důvěra mezi pracovníky úřadu	Slabé fyzické zabezpečení
Kvalitní správce PC sítě	Absence dlouhodobé strategie rozvoje IS
Dobrá technologická infrastruktura IS	Zastaralý hardware
Podpora zastupitelů v bezpečnostní politice	Absence záložního zdroje
Příležitosti	**Hrozby**
Rozšířené využití elektronické spisové služby	Dlouhodobý výpadek elektrické sítě
Rozšířit a zabezpečit vnitřní WIFI pokrytí	Nedostatečná ochrana proti průniku škodlivého kódu
Výměna serveru za rychlejší a bezpečnější	Kyberútok, napadení ransomwarem
Sdílet zkušenosti s jinou obcí	Porucha hardware vedoucí ke ztrátě dat
Elektronizace poplatků za odvoz odpadu	Dlouhodobá nemoc správce sítě

Tabulka 1. SWOT analýza, vlastní zpracování

Závěry vyplývající z šetření v obcích Hornolidečska

Jak zabezpečit lokální síť po stránce technické, organizační nebo personální je popsáno v mnoha odborných publikacích. Reálný stav v malých obcích je mnohdy daleko od těchto popsaných ideálů. Dotazníkové šetření a rozhovory se starosty ukazují na skutečný stav zabezpečení eGovernmentu. Z těchto rozhovorů vyplývá, že starostové mají jen omezený přehled o tom, co vše zahrnuje eGovernment v místní samosprávě a jak ho správně zabezpečit. Vlastní shrnutí uvádím níže:

Starostové mají malé povědomí v oblasti zabezpečení eGovernmentu.

Bez základního přehledu a orientace v oblasti elektronické a kybernetické bezpečnosti bude starosta jen těžko dohlížet na oblast bezpečnosti informačního systému (za kterou mimo jiné také zodpovídá). Základní orientaci přináší příručka pro starosty: „Jak se vyznat v eGovernmentu“, která je v příloze této práce. Další zdroje jsou uvedeny ve 4. kapitole (Vzdělávání).

Starostové nekriticky spoléhají na své správce počítačových sítí.

Pokud není starosta z IT oboru, je odkázán ve svém úsudku na správce počítačové sítě na obci. V současné době rostou nároky na zabezpečení informačního systému obce. Správce počítačové sítě je klíčová osoba v oblasti zabezpečení informačního systému. Pokud je odborně zdatný, dokáže informační systém optimálně zabezpečit. Co ale v případě, že není? Starostové podle mě až příliš důvěřují správcům sítě, že nastavení prvků v síti je optimální.

Starostové vnímají zavádění eGovernmentu jako další zátěž na chod úřadu.

Je velký rozdíl v úrovni zavedení eGovernmentu na OÚ malých obcích. Některé obce se teprve chystají na zavedení elektronické spisové služby. Někde přežívá dvojí evidence papírová i elektronická. Zaznívají hlasy o přetížení zaměstnanců dalšími úkoly spojenými s elektronizací veřejné správy (obsluha nového softwaru, poskytování nových služeb na úřadě, např. Czech POINT). I když starostové nakonec připouštějí, že po zvládnutí nových výzev se stávají elektronické nástroje jejich pomocníky. Novým úkolem, který musely zvládnout i malé obce, bylo (rok 2018) zavedení funkce pověřence pro ochranu osobních údajů. Většina obcí má externího pověřence. Zavedení pověřence není jen splnění legislativní povinnosti, ale má význam pro všechny klienty veřejné správy. Obec může dále využít

pověřence jako školitele svých zaměstnanců a také ho zapojit do systému zabezpečení informačního systému. Pověřenec totiž dohlíží na bezpečnost osobních údajů v organizaci a měl by se orientovat v základech IT technologií i ve způsobech zabezpečení dat na obci. Jako druhá nezávislá osoba může posoudit stav zabezpečení informačního systému obce. V ideálním případě tak může zastat roli správce bezpečnosti informačního systému. Tím získá obec dvojí kontrolu, neboli základní bezpečnostní princip "čtyř očí", který eliminuje množství chyb v rozhodování.

Starostové si uvědomují závislost eGovernmentu na elektrické energii.
Mnozí starostové si uvědomují potřebu záložního zdroje. Současný růst cen energií (rok 2021/2022) možná pomůže v rozhodování pořídit pro obecní úřad záložní zdroj. Fotovoltaická elektrárna na střeše budovy obecního úřadu s bateriovým úložištěm může zajistit úřadu úsporu energie i potřebnou zálohu energie v případě výpadku elektrické proudu.

Nebezpečí v dostupnosti elektronických služeb pro některé občany.
Starostové ze tří obcí se nezávisle na sobě shodli na tom, že další pokračování digitalizace může mít negativní vliv na přístup některých skupin občanů ke službám eGovernmentu. Problémem může být nedostupnost těchto technologií pro starší a sociálně slabé lidi. Tyto skupiny budou prakticky vyřazeni z možnosti využívat elektronickou komunikaci s úřady i z důvodu malé počítačové gramotnosti. K tomuto tématu více v kapitole 3.1 (Sociální hrozby).

Na základě těchto podnětů od starostů jsem v rámci této práce navrhl **Standard zabezpečení pro malé obce (viz kapitola 7)**, který má být takovým minimálním odrazovým můstkem pro bezpečnost eGovernmentu. Tyto informace mohou sloužit k určení oblastí, které by měly mít obce dostatečně zabezpečeny. Každá obec má své slabé stránky bezpečného fungování eGovernmentu. Standard zabezpečení pro malé obce definuje prvky zabezpečení, které by neměly být opomenuty při posilování bezpečnosti informačního systému obce.

6.3. Zabezpečení informačního systému obce

Zjištění současného stavu je důležité pro určení toho, kde se právě nacházíme. Současně musíme mít představu, kam se chceme posunout (to znamená, jaký je ideální stav). Ideální stav zabezpečeného informačního systému obecního úřadu si definujme:

- **Zabezpečený proti vnějším hrozbám**
- **Zabezpečený proti vnitřním hrozbám**

Rozdělení na vnější a vnitřní hrozby bylo popsáno v 3. kapitole (Rizika eGovernmentu ve státní správě). Vnější hrozby se malých obcí týkají jen okrajově. Zabezpečení proti vnějším hrozbám se zajistí na úrovni technické infrastruktury lokální sítě. Co se týká vnitřních hrozeb, chráněným aktivem v informačním systému obce jsou data (elektronické informace). V podmínkách malých obcí tak zabezpečení dat znamená řešit tyto čtyři prvky: fyzická bezpečnost všech prostor obecního úřadu, technická infrastruktura lokální sítě, používaný aplikační software, poučená obsluha.

Opatření proti vnitřním hrozbám znamenají zajistit fyzickou bezpečnost všech prostor obecního úřadu, mít vystavěnu lokální síť z kvalitních prvků, spolupracovat s kvalitním správcem sítě, nastavený bezpečný firewall, antivirový program, používat pouze nezbytné a důvěryhodné aplikace, které využívá poučená obsluha.

K zabezpečení místního eGovernmentu je třeba přistupovat komplexně a jak se říká se "selským rozumem". Příkladem nepromyšlených opatření může být pořízení agregátu, který při výpadku napájení sice naskočí, ale vyrobí v síti takové přepětí, že vypadnou všechny pojistky. Za další příklad podcenění zabezpečení může sloužit instituce s názvem Národný bezpečnostný úrad Slovenskej republiky (NBU SR). V roce 2006 se skupině hackerů podařilo proniknout do e-mailového systému této organizace, která má bezpečnost přímo ve svém názvu. Nebylo to zvlášť obtížné, přihlašovací jméno bylo NBUSR a heslo NBUSR123.[56]

[56] VODIČKA, Milan. 3D: *Data, daně digitálně, aneb, Ajťákem i proti své vůli*. Praha: Wolters Kluwer, 2014., (s.175)

Řízení bezpečnosti informačního systému obce

Pro správné nastavení bezpečnosti informačního systému je zapotřebí mít definovány požadavky v písemné podobě. Takový systém již existuje v komerční sféře. Podobně můžeme postulovat bezpečnostní dokumenty i ve veřejné správě.

„Pro účinné vynucení bezpečnostních opatření organizační a technické povahy je nutné, aby veškeré požadavky byly dokumentovány. Určité bezpečnostní zásady jsou často formulovány v bezpečnostní politice, standardech a příručkách. Ačkoliv je mezi těmito dokumenty podstatný rozdíl, jsou velice často zaměňovány. Dokumenty, ve kterých jsou bezpečnostní zásady formovány, jsou pouze určitým předpokladem k dosažení požadované úrovně bezpečnosti. Takže jestli to myslíte s bezpečností opravdu vážně a chcete, aby zásady v těchto dokumentech uvedené byly vašimi zaměstnanci v praxi dodržovány, měli byste je formulovat tak, aby pro ně byly srozumitelné a mohli se jimi opravdu řídit a dodržovat je.“[57] Rozlišujeme dokumenty podle hierarchie na strategické dokumenty (policy), standardy a procedury.

Bezpečnostní politika je strategický dokument, který definuje účel, cíl a záměr společnosti v oblasti bezpečnosti. Jedná se o jasný a srozumitelný způsob, kterým management dává najevo svůj záměr prosazovat informační bezpečnost a dodržování zásad všemi zaměstnanci, neboť si je vědom rizik, kterým společnost musí čelit. Kromě toho může obsahovat i obecné požadavky, např. že uživatelé mají používat silná hesla. Požadavky uvedené v bezpečnostní politice by měly být dále rozpracovány ve formě bezpečnostních standardů. V politice by měly být používány jasné formulace – musí, nesmí. Bezpečnostní politika by nám měla především odpovědět na otázku, proč to děláme.

Standard je taktický dokument, který rozpracovává obecné požadavky uvedené v bezpečnostní politice. Měl by již definovat naprosto konkrétní a detailní požadavky, např. jaké služby mají běžet na serveru a jaké na něm naopak běžet nesmí, jak má být nastaveno logování, jakých hodnot mají nabývat určité parametry

[57] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. (s. 98)

(např. že heslo musí obsahovat velká a malá písmena, čísla, speciální znaky a musí být dlouhé minimálně 15 znaků). Bezpečnostní standardy by nám měly poskytnout odpověď na otázku, co se má udělat.

Procedury jsou provozní dokumenty, které krok za krokem popisují, jak provádět určitou činnost nebo zavést konkrétní opatření. Cílem je, aby byl konkrétní proces dostatečně popsán a tak bylo minimalizováno riziko chyby. Procedury mohou obsahovat detailní postup, jak např. nastavit systém, nainstalovat nějakou komponentu, aktivovat politiku vynucující bezpečná hesla. Procedury nám tedy přinášejí odpověď na otázku, jak splnit požadavky uvedené ve standardu.

Vztah mezi těmito třemi základními dokumenty je zachycen na následujícím obrázku.[58]

Obrázek 19. Vztah mezi základními bezpečnostními dokumenty. (KNÝ, Milan a Josef POŽÁR)

[58] KNÝ, Milan a Josef POŽÁR. *Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti.* Brno: Tribun EU, 2010.

7. Zabezpečení eGovernmentu v malých obcích

Následující Standard zabezpečení pro malé obce je takovým příkladem taktického dokumentu pro malé obce. Samozřejmě bude potřeba si seznam upravit podle specifických místních podmínek. Avšak zmíněné oblasti bezpečnosti se s největší pravděpodobností budou objevovat v každém konkrétním IS.

7.1. Standard zabezpečení IS malé obce:

1) Máme plán údržby a obnovy informačního systému úřadu.

Není třeba mít dokonalé mnohastránkové směrnice o bezpečnosti, které nikdo nečte a nic z toho se nepoužívá. Každá vnitřní směrnice, pokud si ji úřad schválí, by měla být závazná. Stačí ale jednoduchý předpis toho, co je třeba v systému posílit, popis odpovědností, systém zálohování dat, plán činnosti v případě napadení systému apod.

2) Máme dostatečně zabezpečené fyzické prostory úřadu.

Máme dobře zabezpečenou budovu obecního úřadu? Zvážili jsme napojení na pult centrální ochrany (např. firma ANIM plus, Vsetín), kamerový systém, bezpečnostní dveře apod.? Jsou dveře do místnosti se serverem zamknuté a přístupné jen příslušné osobě? Máme přehled o pohybu osob na úřadě? Nezůstávají dveře do kanceláře otevřené, když v místnosti nikdo není? S technikou, kterou používáme (notebook, mobil) zacházíme tak, aby se eliminovaly možnosti odcizení.

3) Pravidelně zálohujeme a jednu zálohu uchováváme mimo budovu.

V rámci zálohování je doporučeno řešit i uložení médií, na která se zálohování provádí. Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3-2-1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění informačního systému.

4) **Udržujeme software i operační systém aktuální.**

Správce systému musí pravidelně kontrolovat všechny prvky systému a zajistit jejich aktuálnost. Týká se to hlavně operačního systému a antivirového programu. Nesmí se také zapomenout ani na aktuální firmwary síťových prvků.

5) **Používáme antivirový program a firewall.**

Absolutní nezbytností je aktualizovaný antivirový program. Například produkt od firmy ESET Internet security dokáže kromě antivirové ochrany zajistit také dodatečnou ochranu. Chrání online platby a přístup do elektronického bankovnictví. Šifruje komunikaci mezi klávesnicí a prohlížečem, aby specifický malware (keylogger) nemohl získat citlivá data typu hesel a podrobností o kreditních kartách. Funguje jako firewall. Brání neautorizovaným uživatelům v přístupu na zařízení a zneužití osobních dat. Upozorní uživatele na nevyžádané použití webové kamery. Umožňuje také otestovat domácí router a připojená chytrá zařízení na různé zranitelnosti. Odhalí podvodné internetové stránky, jež se snaží získat citlivá data, jako jsou uživatelská jména, hesla nebo bankovní údaje.

6) **Přihlašujeme se heslem do PC.**

I když si na obecním úřadě důvěřujeme, měly by být počítače chráněny heslem. Je to z toho důvodu, že nevíme, kdo jiný může mít přístup k našemu PC. Při odchodu od počítače se ubezpečíme, že jsme se odhlásili. Svá hesla neuchováváme na lístečcích nalepených na monitoru. Používáme pokud možno vícefaktorovou autentizaci do svých aplikací.

7) **Cizí paměťová media používáme na PC mimo lokální síť.**

Cizí paměťové médium (nejčastěji USB flash disk) může být zavirován nebo obsahovat škodlivý kód. Antivir by měl tyto nástrahy zlikvidovat, přesto se na něj nemůžeme na 100 % spolehnout. Aby nedošlo k napadení ostatních počítačů v síti, je doporučeno provádět operace s cizími médii na počítači, který není zapojen v síti (například notebook).

8) **Pravidelně školíme obsluhu počítačů.**

Pro všechny zaměstnance by měla být stanovena pravidelná školení týkající se základů kybernetické bezpečnosti (a to minimálně 1× ročně). Při výskytu

mimořádné události (např. nová obecně známá hrozba) je vhodné zorganizovat mimořádné školení, případně zaměstnance informovat jiným vhodným způsobem.

9) **Správce PC sítě má naši důvěru.**

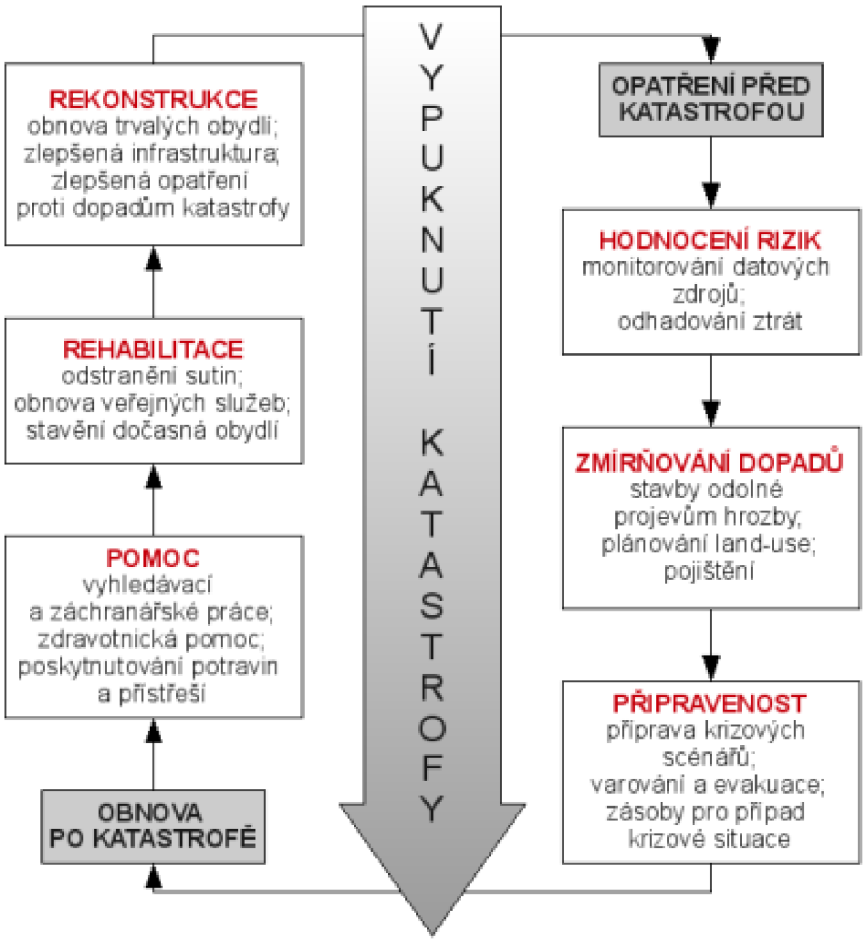
Správce počítačové sítě dobře vybíráme. Pokud nemá dostatečnou kvalifikaci nebo mu nemůžeme důvěřovat, raději se poohlédneme po někom jiném. Správce sítě má největší vliv na to, jak je náš informační systém odolný. Má také přístup (hesla) do serveru a síťových prvků. To je obrazně, jako by měl klíče od obecního úřadu.

10) **Máme informační systém zajištěn záložním zdrojem.**

Bez elektrické energie není ani eGovernment. Obecní úřad by měl být vybaven záložním zdrojem pro případ dlouhodobého výpadku elektrické energie. Dobrým řešením může být fotovoltaická elektrárna se záložními bateriemi (lze pořídit i za pomocí dotace), která zároveň šetří náklady na provoz úřadu. Při současných cenách energií se náklady na pořízení fotovoltaické elektrárny vrátí řádově do několika let.

Kdo je připraven, není překvapen

Ekonomové říkají, že krize jsou nevyhnutelné. Otázkou není, jestli přijdou, ale kdy přijdou. Proto je dobré na informační systém místní správy hledět jako na nekončící proces vyhodnocování rizik, provádění preventivních opatření a řešení následků po incidentu. Obrazně se na tenko koloběh můžeme dívat optikou zvládání přírodních katastrof. Před přírodní katastrofou (ale i před bezpečnostním incidentem) monitorujeme náš informační systém a zajišťujeme slabá místa proti možným hrozbám. Aktualizujeme firmware přístrojů, vyměňujeme zastaralé prvky komunikační infrastruktury, hardware i software udržujeme aktuální. Máme připravený rizikový plán, pro případ narušení systému. Pravidelně zálohujeme a kontrolujeme, zda jsou zálohy použitelné. V případě kybernetického napadení nebo jiného incidentu víme, koho máme přizvat k řešení problému.



Obrázek 20. Obnova po katastrofě, dostupné z https://sites.google.com/site/teoretickavychodiska/predpoved_ochrana_obnova [cit. 2022-03-16]

A pokud dojde k napadení systému nebo ke ztrátě dat, měli bychom mít stručný manuál, co v takovém případě dělat. „Obvykle se postupuje podle následujícího scénáře:

- Identifikovat, kde k bezpečnostnímu incidentu došlo
- Co nejvíce zamezit dalším škodám
- Analyzovat příčinu a zajistit stopy pro další analýzu
- Odstranit příčinu a obnovit funkčnost
- Zhodnotit škody
- Iplementovat vhodná opatření k zamezení opakování incidentu
- Seznámit ostatní s výsledky šetření“[59]

[59] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. (s. 260)

V praxi bývá často zanedbaná analýza příčin, protože vedení organizace většinou požaduje rychlou obnovu provozu, a na zajištění důkazů a zjištění příčin tak nezbývá čas. Ignorováním analýzy příčin však velmi omezíme možnosti navržení a implementaci vhodných opatření pro zamezení opakování incidentu.

Předcházení ztráty dat

Pokud máme zabezpečenou počítačovou síť podle standardu zabezpečení, můžeme se věnovat prevenci možných hrozeb. Na to existuje několik nástrojů. Nezmar (2019) zmiňuje například systém prevence průniku (Intrusion Prevention Systém, zkratka IPS), který monitoruje síť na škodlivou činnost. Další nástroj je systém DLP (Data Loss Prevention). Rozlišujeme dva druhy DLP řešení. Síťová DLP pomáhají zabránit úniku citlivých dat na úrovni vnější komunikace společnosti. Endpoint DLP naproti tomu brání úniku dat z jednotlivých pracovních stanic organizace. DLP systémy jsou významným pomocníkem především při ochraně před ztrátou dat způsobených vlastními zaměstnanci. DLP systémy jsou schopny efektivním způsobem zajistit odpovídající politiku přístupu k datům. K údajům pustí jen ty, kteří jsou oprávněni a zajistí využití dat pouze požadovaným způsobem. Do značné míry tak lze eliminovat selhání lidského faktoru. Nasazení DLP systému není všelék. Systém nedovolí uživateli data vytisknout nebo zkopírovat. Dá se to ale obejít tím, že údaje může uživatel vyfotit telefonem z obrazovky.

„Náklady spojené se ztrátou dat se liší dle odvětví. Ve službách hovoříme o nákladu ve výši cca 5 000 Kč na záznam, ve světě financí pak o částce necelých 5,5 tisíc Kč a nejdražší jsou záznamy ve zdravotnictví, kde náklad na jeden řádek databáze vychází na téměř 8,5 tisíc Kč. Studie uvádí, že každá čtvrtá organizace se již s porušením integrity dat setkala. Studie mimo jiné ukazuje, že existuje přímá úměra mezi dobou, kdy dojde k odhalení porušení dat, a náklady s tím spojenými. Jednoduše platí, že čím později tím dražší.“ [60]

[60] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. (s. 264)

Závěr

Tato práce nejprve představila systém veřejné správy v České republice a jeho vývoj směrem k elektronickému vládnutí, tedy eGovernmentu. Vývoj elektronizace veřejné správy odráží širší trend v pojetí veřejné správy jako služby občanům. Česká republika schválila v nedávné době klíčovou legislativu v oblasti eGovernmentu. To otvírá dveře rozvoji eGovernmentu a většímu využití elektronické komunikace mezi veřejnou správou a občany. S legislativním zakotvením elektronické identity občana se rozvoj služeb eGovernmentu (i komerčních služeb) ještě rozšíří.

eGovernment v samosprávě má svá specifika oproti eGovernmentu ve státní správě. Kromě portálu občana obce (přihlašování prostřednictvím Identity občana) je málo vztyčných bodů se státní správou. Obce komunikují elektronicky s občany prostřednictvím svých www stránek. K tomu ještě přistupují různé interaktivní aplikace a sociální média. V prostředí obecního úřadu je pak největší pozornost věnována zabezpečení informačního systému a bezpečnosti uložených dat. Informační systém obecního úřadu musí být chráněn nejenom před externími hrozbami, ale i interními hrozbami. Mnohé rizika se sníží, pokud je dobře poučena obsluha informačního systému.

Klíčová část práce se věnuje rizikům eGovernmentu a jeho zabezpečení především na úrovni malých obcí. Jsou uvedeny konkrétní doporučení a postupy, která mohou pomoci starostům těchto obcí bezpečně zvládnout digitalizaci na svých úřadech. Průzkum stavu eGovernmentu v obcích Hornolidečska spolu s názory samotných starostů ukazují skutečný stav eGovernmentu v malých obcích. Dotazníkové šetření svým rozsahem není reprezentativní vzorek pro celou Českou republiku. Přesto může poskytnout obraz eGovernmentu v těchto obcích. Ze zjištěných skutečností a studia odborné literatury bylo možné sestavit doporučení pro zabezpečení jejich informačních systémů. Standard zabezpečení informačního systému malé obce shrnuje nejdůležitější aspekty této bezpečnosti. Doporučení, která jsou v této práci předkládaná, mohou pomoci také ostatním malým obcím napříč republiky. Jedním z výstupů této práce je příručka pro starosty, která dává svým čtenářům základní orientaci v oblasti eGovernmentu.

Použité zdroje

Knižní zdroje

[1] ALVAROVÁ, Alexandra. *Průmysl lži: propaganda, konspirace a dezinformační válka*. Praha: Stanislav Juhaňák - Triton, 2017. ISBN 978-80-7553-492-7.

[2] HENDRYCH, Dušan. *Správní věda: teorie veřejné správy*. 4. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-561-0.

[3] KNÝ, Milan a Josef POŽÁR. *Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti*. Brno: Tribun EU, 2010. ISBN 978-80-7399-067-1.

[4] LIDINSKÝ, Vít. *EGovernment bezpečně*. Praha: Grada, 2008. ISBN 978-80-247-2462-1

[5] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.

[6] PROVAZNÍKOVÁ, Romana. *Financování měst, obcí a regionů: teorie a praxe*. Praha: Grada, 2007. ISBN 978-80-247-2097-5.

[7] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[8] ŠPAČEK, David. EGovernment: cíle, trendy a přístupy k jeho hodnocení. V Praze: C.H. Beck, 2012. ISBN 978-80-7400-261-8.

[9] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[10] VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-671-6.

[11] VOSTRÁ, Lenka, Jarmila ČERMÁKOVÁ a Jiří GROSPIČ, ed. *Reforma veřejné správy v teorii a praxi: problémy reformy veřejné správy v České republice, Maďarské republice, Polské republice a Slovenské republice: sborník z mezinárodní konference: Třešť, 22.-24. října 2003*. Plzeň: Aleš Čeněk, 2004. ISBN 80-86473-71-6.

[12] ZAKARIA, Fareed. *Budoucnost svobody*. Praha: Academia, 2004. ISBN 80-200-1285-0.

Elektronické zdroje

1. **Aldous Huxley: Konec civilizace**, dostupné z https://www.odaha.com [cit. 2022-03-16]
2. **Architektonická vize eGovernmentu ČR**, dostupné z https://archi.gov.cz [cit. 2022-03-16]
3. **Audit národní bezpečnosti**, dostupné z https://www.vlada.cz [cit. 2022-03-16]
4. **Biden vyzval v telefonátu Putina, aby zasáhl proti hackerům v Rusku**, dostupné z https://www.irozhlas.cz [cit. 2022-03-16]
5. **BIS**, dostupné z https://www.bis.cz/kyberneticka-bezpecnost/ [cit. 2022-03-16]
6. **Cloud vs. on-premise: Jaká je budoucnost?,** dostupné z https://www.totalservice.cz [cit. 2022-03-16]
7. **Co je eGovernment?,** dostupné z: https://www.mvcr.cz/ [cit. 2022-03-16]
8. **Czech POINT**, dostupné z https://www.czechpoint.cz/public/verejnost/sluzby/ [cit. 2022-03-16]
9. **Český statistický úřad**, dostupné z https://www.czso.cz [cit. 2022-03-16]
10. **Čína zavádí sociální kreditní systém**, dostupné z https://www.businessinfo.cz [cit. 2022-03-16]
11. **Data v cloudu, data v čoudu**, dostupné z https://www.cleverandsmart.cz [cit. 2022-03-16]
12. **Digitální Česko**, dostupné z https://www.digitalnicesko.cz/zakladni-informace [cit. 2022-03-16]
13. **Digitální úřad**, dostupné z https://digitalni-urad.cz/#/ [cit. 2022-03-16]
14. **eGon**, dostupné z https://www.mvcr.cz/ [cit. 2022-03-16]
15. **eGovernment cloud**, dostupné z https://archi.gov.cz/nap:egovernment_cloud [cit. 2022-03-16]
16. **Evropě hrozil masivní blackout**, dostupné z https://www.idnes.cz [cit. 2022-03-16]
17. **Historie digitalizace služeb**, dostupné z https://archi.gov.cz/znalostni_baze:historie_egov [cit. 2022-03-16]

18. **Hornolidečsko**, dostupné z http://www.hornolidecsko.cz/cz/1-clenske-obce.html [cit. 2022-03-16]
19. **Identifikace v informačních systémech**, dostupné z https://https://archi.gov.cz/ [cit. 2022-03-16]
20. **Identita občana**, dostupné z https://www.identitaobcana.cz/ [cit. 2022-03-16]
21. **Informační koncepce ČR**, dostupné z https://archi.gov.cz/ikcr [cit. 2022-03-16]
22. **Iniciativa 202020**, dostupné z https://www.202020.cz/ [cit. 2022-03-16]
23. **Kauza Vrbětice**, dostupné z https://cs.wikipedia.org [cit. 2022-03-16]
24. **Kybertest**, dostupné z https://kybertest.cz/projektu [cit. 2022-03-16]
25. **Blackout v Severní Americe (2003),** dostupné z https://cs.wikipedia.org [cit. 2022-03-16]
26. **NAKIT**, dostupné z https://nakit.cz/o-agenture-nakit/ [cit. 2022-03-16]
27. **Národní architektonický plán**, dostupné z https://archi.gov.cz/start [cit. 2022-03-16]
28. **Národní plán obnovy**, dostupné z https://www.planobnovycr.cz/pilire [cit. 2022-03-16]
29. **NUKIB**, dostupné z https://www.nukib.cz/cs/ [cit. 2022-03-16]
30. **NUKIB, Vzdělávání**, dostupné z https://www.nukib.cz/ [cit. 2022-03-16]
31. **Osobní portál občana**, dostupné z https://gordicportalobcana.cz/varianty/ [cit. 2022-03-16]
32. **Policie dopadla skupinu hackerů, která útočila na benešovskou nemocnici a OKD**, dostupné z https://ct24.ceskatelevize.cz [cit. 2022-03-16]
33. **Rada vlády pro informační společnost**, dostupné z https://www.mvcr.cz [cit. 2022-03-16]
34. **Systém sociálního kreditu**, dostupné z https://cs.wikipedia.org [cit. 2022-03-16]
35. **Systém veřejné správy v ČR**, dostupné z https://icv.vlada.cz/ [cit. 2022-03-16]

36. **Ty knihy je potřeba zničit!,** dostupné z https://www.seznamzpravy.cz [cit. 2022-03-16]
37. **UOOU**, https://www.uoou.cz/ [cit. 2022-03-16]
38. **USA a další země zasáhl masivní kybernetický útok**, dostupné z https://www.irozhlas.cz [cit. 2022-03-16]
39. **Utopie**, dostupné z https://encyklopedie.soc.cas.cz/w/Utopie [cit. 2022-03-16]
40. **WannaCry**, dostupné z https://www.avast.com [cit. 2022-03-16]
41. **Základní registry a Správa základních registrů**, dostupné z https://www.mvcr.cz/ [cit. 2022-03-16]

Legislativa

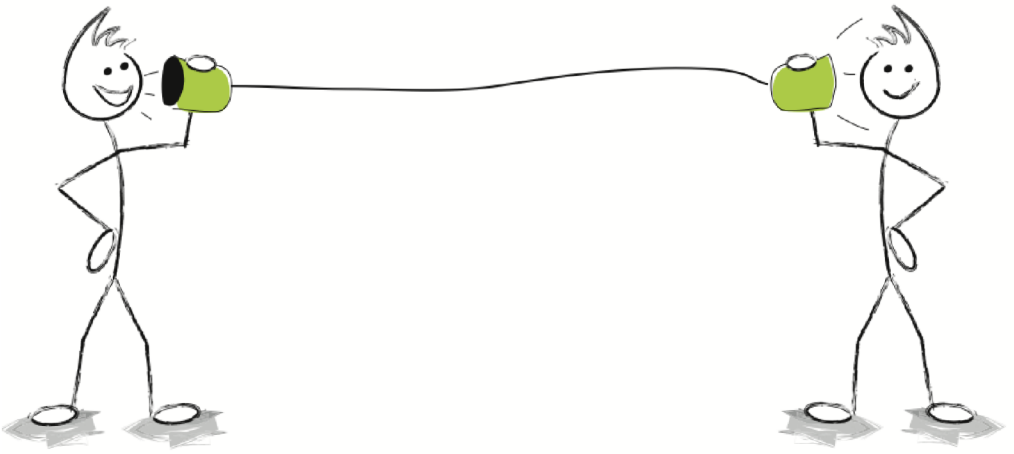
- Zákon č. 1/1993 Sb., Ústava ČR
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Zákon č. 111/2009 Sb., o základních registrech
- Zákon č. 12/2020 Sb., o právu na digitální službu
- zákon č. 123/1998 Sb., o právu na informace o životním prostředí
- zákon č. 123/1998 Sb., o právu na informace o životním prostředí
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 200/1994 Sb., o zeměměřictví
- Zákon č. 250/2017 Sb., o elektronické identifikaci
- Zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)
- Zákon č. 261/2021 Sb., Zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 500/2004 Sb., Správní řád

Seznam obrázků

Seznam tabulek

Příloha

Příručka pro starosty



Jak se vyznat v eGovernmentu

Úvod

Český filozof, profesor Václav Bělohradský, v knize rozhovorů s Karlem Hvížďalou říká, že: „Tvořivou lidskou prací změněný svět je takový svět, v kterém je:

- Vše je reprodukovatelné.
- Vše je instalovatelné.
- Vše je mobilní.

Tato slova znějí dnes obyčejně, ale v roce 1985, kdy tento rozhovor vznikal, jsou to slova prorocká. Dnes, po více jak 30 letech, slovo "mobilní" běžně používáme. Zvykli jsme si na to, že přístup k informacím můžeme mít hned a také odkudkoliv. Díky internetu můžeme využívat největší knihovnu na světě, ale také spotřebovávat různé formy multimediální zábavy. Můžeme také využívat komerční služby (e-shopy), ale i služby veřejné správy. Díky internetu můžeme ovládat "svůj svět" z pohodlí obýváku nebo třeba přes mobil. Jsme dostupnější díky sociálním sítím a videohovorům, ale také více vystaveni různým dezinformacím a sofistikovaným nástrojům na sběr dat na internetu pod správou velkých korporací jako je Google nebo Facebook (viz např. aféra Cambridge Analytica). Do jakého světa se budeme probouzet zítra? Je zřejmé, že kromě identity ve fyzickém světě, se budeme prokazovat svou identitu i v tom virtuálním světě. A podobně jako zanecháváme svou "stopu" v tom fyzickém světě, budeme takovou stopu zanechávat i v tom virtuálním. A ta bude stejně reálná. A stejně tak jako jsou zloději v reálném světě, zkouší to i v tom virtuálním. A někdy si přijdou i na takové peníze, které by v tom reálném jen stěží unesli. V tomto e-booku se zaměříme na to, aby náš pohyb ve virtuálním světě byl, jak říkají někteří lidé "hlavně bezpečný". A o to jde, buďme mobilní a zůstaňme v bezpečí.

1. Co je to eGovernment?

Slovo eGovernment se stalo často skloňované v oblasti reformy veřejné správy. Veřejná správa se dělí na státní správu a samosprávu. Státní správa i samospráva mají být díky elektronizaci efektivnější, rychlejší a dostupnější. Slovo eGovernment nemá v češtině svůj ekvivalent, jeho doslovný překlad znamená "elektronická vláda". Pojem eGovernment má přesah do různých vědních disciplín jako je informatika, kybernetika, politologie či právo. Spíše než o technický pojem se jedná o politický termín. Používají ho politické strany na ideologické škále zleva doprava. Vzhledem k poměrně dobré dostupnosti internetu u nás, je poptávka po eGovernmentu výrazně tlačena ze strany uživatelů, tedy občanů. Rozvoj

eGovernmentu má své výhody i rizika spojená s nebezpečím ztráty dat a s nebezpečím zneužití dat (bodový systém občanů v Číně).

1.1. Zákon o právu na digitální službu

„Digitalizace veřejné správy je v České republice zatím velmi pozvolná, ale postupně nabírá na obrátkách. Významně přispět k tomu může i Zákon o právu na digitální služby z roku 2020, který dává občanům právo požadovat po státu digitální služby kdykoli, když není pádný důvod pro fyzickou návštěvu úřadu. Navíc občany zbavuje povinnosti poskytovat údaje, kterými již stát disponuje. Tím bude ušetřen čas a úsilí na obou stranách, protože interaktivní formulář předvyplní již dříve sdílená data místo občana.“[1]
Zákon o právu na digitální služby 12/2020 Sb. je někdy označován také jako digitální ústava. Zákon stanovuje, že občan může požadovat po státu veškerou komunikaci elektronicky a stát má povinnost digitální službu poskytnout (§ 3). Stát může požadovat po občanovi údaje jen jednou (tedy ty údaje, které občan státu ještě neposkytl). Orgán veřejné moci nevyžaduje údaje vedené v základním registru nebo agendovém informačním systému, které jsou mu zpřístupněné pro výkon agendy nebo na základě souhlasu uživatele služby (§7). V praxi by to mohlo vypadat tak, že namísto více než 260 různých průkazů a dokladů (občanský průkaz, řidičský průkaz, průkaz pojištěnce, tramvajenka, zbrojní pas, rybářský lístek, …), které v Česku existují, bychom vždy předložili pouze jen elektronický občanský průkaz uložený třeba v mobilním telefonu, jako to mají v Estonsku, a to by bylo vše.

Vyjmuty z povinnosti poskytovat digitální službu byly územní samosprávné celky – obce a kraje, povinnost poskytovat digitální službu jim zůstala pouze pro služby přenesené působnosti.

Přínosy zákona:

- Poskytovatel digitální služby musí uchovávat záznam o digitálním právním jednání občana.
- Pokud není předem zveřejněn elektronický formulář nebo předem stanoven způsob elektronického jednání vůči úřadu, občan má právo učinit podání v jakémkoli formátu poslaném přes datové schránky.

[1] Digitální úřad, dostupné z https://digitalni-urad.cz/#/ [cit. 2022-03-16]

- Po identifikaci občana má tento právo, aby se mu automaticky do interaktivních formulářů vyplnily ty údaje, které už o občanovi stát má.
- Občan má mít právo přístupu ke všem informacím, které o něm stát vede.
- Pokud občan službu v digitální podobě nedostane, může ji vymáhat soudně.

2. eGovernment ve státní správě

Díky eGovernmentu mohou být některé služby státní správy otevřené 24 hodin denně, tedy přístupné on-line. U ústředních státních orgánů jsou služby eGovernmentu přístupny prostřednictvím tzv. portálů, což jsou webové stránky organizace, kde lze různá podání vyřídit elektronicky, například:

- Daňový portál
- Portály zdravotních pojišťoven
- Portál ČSSZ
- Portál justice

Do portálu se může přihlásit každý občan třeba z pohodlí domova. Podmínkou je přístup na internet a také je třeba mít zřízenu datovou schránku nebo identitu občana (dříve eIdentita).

Obrázek 1: Přihlášení do portálu mojedaně.cz , dostupné z (https://adisspr.mfcr.cz/pmd/home/prihlaseni-do-dis) [cit. 2022-03-16]

Obrázek 2: Portál ČSSZ, dostupné z https://eportal.cssz.cz/web/portal [cit. 2022-03-16]

2.1. Elektronická identita

Elektronická identita je klíčem, který otvírá dveře (portál) k využívání elektronických služeb. Je několik způsobů identifikace, jak vydávaných státem, tak soukromoprávními poskytovateli.

- Občanský průkaz s aktivovaným kontaktním elektronickým čipem vydaný po 1. 7. 2018 je prostředkem na vysoké úrovni záruk.
- Národní identifikační autorita (NIA ID) – státem zdarma poskytovaný identifikační prostředek založený na kombinaci jména, hesla a SMS kódu, dříve označovaný jako uživatelský účet, OTP či UPS.
- Mobilní klíč eGovernmentu – státem zdarma poskytovaný identifikační prostředek, který představuje využití přihlašování bez potřeby zadávání dalších ověřovacích kódů.
- Bankovní identita

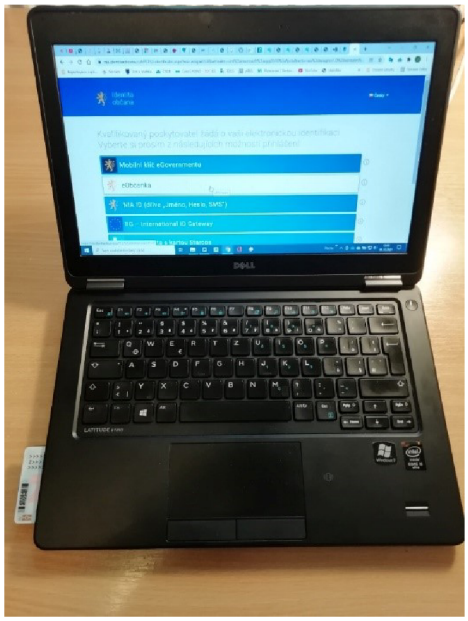
Obrázek 3: identita občana, dostupné z https://www.identitaobcana.cz/Home [cit. 2022-03-16]

Zvolený způsob přihlášení určuje i rozsah služeb, které jsou uživateli přístupné. Rozlišují se tři úrovně záruky (důvěry) identifikačních prostředků: nízká, značná, vysoká. Zjednodušeně řečeno jde o úrovně, jak moc může poskytovatel služby důvěřovat způsobu prokázání totožnosti:

- U vysoké úrovně jde o autentizaci, kdy mám fyzicky identifikační prostředek na bezpečném zařízení (např. na kontaktním čipu občanského průkazu, který mám u sebe), při jeho vydání byla zaručeně ověřena moje totožnost a znám přístupové údaje k jeho použití.
- U značné úrovně (např. NIA ID) jde o tzv. dvoufaktorovou autentizaci – jméno, heslo a jednorázově zasílaný SMS kód. Moje totožnost byla ověřena před aktivací prostředku (na kontaktním místě veřejné správy Czech POINT, prostředkem stejné nebo vyšší úrovně důvěry nebo pomocí datové schránky).
- U nízké úrovně nedošlo k zaručenému ověření totožnosti – zvolím si uživatelské jméno a heslo a svoji identitu pouze deklaruji.

Příkladem identifikace prostřednictvím eObčanky je obrázek níže. Mnohé notebooky mají čtečku karet v sobě zabudovanou, u osobních počítačů je třeba dokoupit USB čtečku karet (cena čtečky začíná na 200 Kč). Do zařízení je třeba dále nainstalovat software eObčanka, kde se zadává 4-místný kód, který jsme si zvolili při vyzvedávání občanského průkazu s čipem na úřadě.

Obrázek 4: Čtečka čipových karet

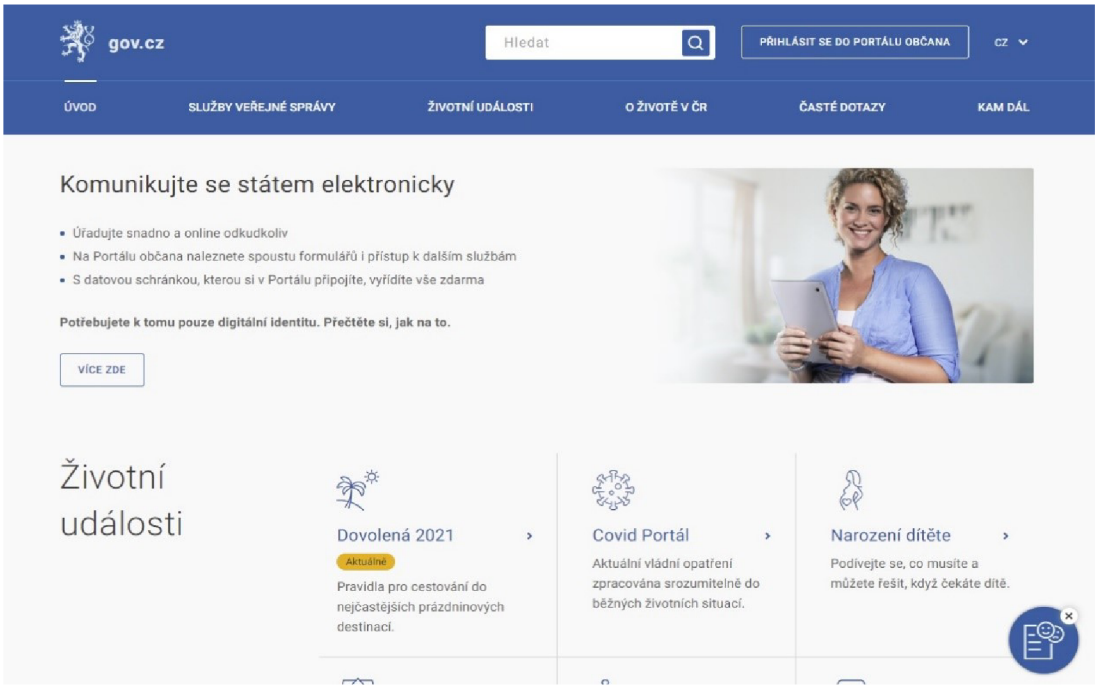


Obrázek 5: Integrovaná čtečka v PC

2.2. Portál veřejné správy

Portál veřejné správy je integrující portál ostatních portálů veřejné správy. Na Portálu veřejné správy je možné se dozvědět nebo vyřídit:

- Informace o životě a podnikání v České republice (důležité pro cizince nebo imigranty)
- Postupy, jak vyřešit životní události (narození dítěte, změna trvalého pobytu, ztráta zaměstnání apod.)
- Přímo využívat služeb veřejné správy (například vyplnit elektronický formulář příspěvku na péči a odeslat ho prostřednictvím datové schránky)
- **Přihlásit se do Portálu občana** a "jít" na úřad konečně on-line (například stáhnout si svůj výpis z rejstříku trestů, podat daňové přiznání nebo zkontrolovat, jaké údaje o mě stát shromažďuje)



Obrázek 6: Portál veřejné správy, dostupné z https://portal.gov.cz/ [cit. 2022-03-16]

Po přihlášení do Portálu občana (v pravém horním rohu) se objeví osobní profil uživatele, s přímým vstupem do datové schránky, s přehledem mých dokladů, údajů vedených o mě v rejstřících a seznam úřadů, kde mohu vyřídit záležitosti on-line.

Obrázek 7: Portál občana, dostupné z https://obcan.portal.gov.cz/ [cit. 2022-03-16]

3. eGovernment v samosprávě

Dostáváme se k eGovernmentu na lokální úrovni. To reprezentují obecní úřady. Ty vykonávají funkci "servisních stanic" své obce (samosprávy), ale zároveň vykonávají (v přenesené působnosti) i státní správu. Malé obce spadají do kategorie obce I. stupně a vykonávají přenesenou působnost v základním rozsahu. Obecní úřad tak sám využívá služeb eGovernmentu, když např. jejich evidence obyvatel se připojí na základní registry a synchronizuje údaje v obecní evidenci s evidencí v registrech. Obecní úřad je i v roli poskytovatele služeb eGovernmentu. Například služby Czech POINT, elektronické informování občanů (např. elektronické hlášení rozhlasu – hlasenirozhlasu.cz) nebo formou zpřístupnění elektronických formulářů na svých webových stránkách. Obecní úřad disponuje většinou malou lokální počítačovou sítí jako informačním systémem. Takový lokální informační systém potřebuje pravidelnou údržbu a technickou podporu. To většinou zastává správce sítě (nejčastěji externí firma). Kromě správce sítě OÚ integruje další funkce, které požaduje aktuální legislativa: pověřenec pro ochranu osobních údajů a administrátor orgánu veřejné moci (OVM). Podívejme se podrobněji na jednotlivé funkce.

Správce sítě

Pokud má obec lokální počítačovou síť, zpravidla má někoho, kdo se stará o bezproblémový chod této sítě. Tento správce sítě by měl být přítomen při návrhu informačního systému a při konfiguraci a zapojení nových prvků do sítě. Měl by mít dokonalý přehled o zabezpečení jednotlivých prvků i celé lokální sítě proti vnějším i vnitřním hrozbám. Správce sítě by měl znát slabiny celého systému a komunikovat se starostou, jakou úroveň zabezpečení má lokální síť splňovat. Správce sítě by měl také zajistit spolehlivé a pravidelné zálohování všech relevantních dat v systému. Požadavky systému by měl stanovit starosta, technické parametry systému by měl řešit správce sítě.

Administrátor orgánu veřejné moci

Institut administrátor orgánu veřejné moci (OVM) byl zaveden s povinností obcí zřídit si datovou schránku podle zákona[2] z roku 2008. Administrátor OVM by neměl být volený zastupitel. Měl by to být zaměstnanec obecního úřadu nebo spolehlivá externí fyzická osoba. Administrátor OVM totiž zpřístupňuje elektronické agendy jednotlivým uživatelům

[2] Zákon 300/2008 Sb., dostupné z https://www.zakonyprolidi.cz/cs/2008-300 [cit. 2022-03-16]

obecního úřadu. Jedná se o centralizované informační systémy jako: informační systém základních registrů a přístup do Czech POINTu. Administrátor zaregistruje do portálu "Czech point/správa dat" vydané přístupové certifikáty nebo elektronické podpisy jednotlivých osob obecního úřadu. Kromě přístupů do centrálních informačních systémů přiděluje jednotlivým uživatelů obecního úřadu tzv. agendové činnostní role. Bez tohoto přidělení by uživatel neměl přístup do agendy, kterou má vykonávat. Jak je vidět, administrátor OVM musí být vysoce spolehlivá osoba, na které závisí důvěryhodnost a bezpečnost dostupných dat v informačních systémech veřejné správy.

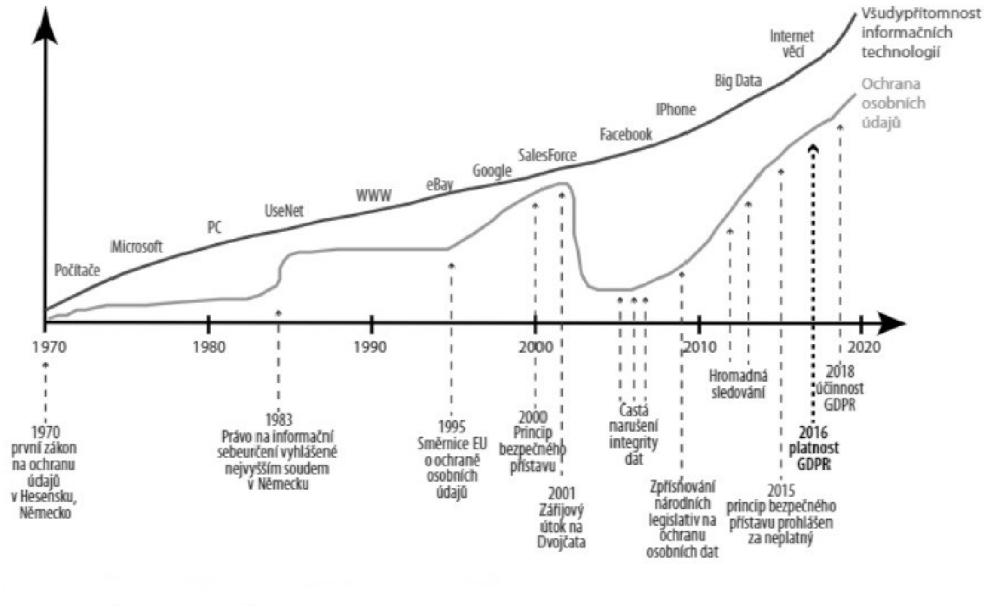
Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je nejmladší funkce spojená s elektronizací obecního úřadu. Funkci pověřence definuje Zákon o ochraně osobních údajů. Pověřenec je "styčným důstojníkem" mezi zpracovatelem osobních údajů (obcí) a osobami, kterých se zpracování týká (občané). V případě bezpečnostních incidentů (ztráta databází týkající se osobních údajů) komunikuje s Úřadem pro ochranu osobních údajů (ÚOOÚ). Provádí poradenství správci či zpracovateli osobních údajů včetně zaměstnanců. Navrhuje opatření k zabezpečení osobních dat a hlídá soulad zpracování osobních údajů (v informačním systému obce) s aktuální legislativou.

3.1. GDPR a ochrana osobních údajů

Náš stát prostřednictvím legislativy proklamuje ochranu osobních údajů. Zákon 110/2019, který implementuje nařízení evropského parlamentu z roku 2016 (GDPR) dává občanům silný nástroj na vymáhání svých osobních práv. Zákon na ochranu osobních údajů má zabránit zneužívání a sbírání osobních údajů pro účely, ke kterým držitel osobních údajů nedal svolení. GDPR se týká také všech obecních úřadů jako zpracovatelů osobních údajů. Nařízení GDPR, kromě zvýšených výdajů z obecní pokladny, obrátilo pozornost starostů k problematice informačních systémů na obecním úřadě a jejich bezpečnosti. Do roku 2018, kdy vstoupilo nařízení v platnost, musely všechny obecní úřady vyhovět požadavkům na ochranu osobních údajů definovaných evropským parlamentem. Šlo to typicky českou cestou, to znamená na poslední chvíli a s pocitem, že nás ta EU zase do něčeho tlačí. Výhody pro nás, uživatele elektronických služeb, jsme viděli až s odstupem. Zákon na ochranu osobních údajů především nastavuje pravidla pro velké zpracovatele

osobních údajů a do určité míry eliminuje jejich zneužití ať už státem, nebo soukromými korporacemi na internetu (Facebook, Google).



Obrázek 8: NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha 2017

Obrázek výše ukazuje, jak se legislativa snaží dohnat překotný vývoj informačních technologií. Graf se týká konkrétně ochrany osobních údajů. Podobně je to však s ostatními oblastmi legislativy a ochrany uživatele vzhledem k novým trendům a technologiím. Legislativa a právo, ať chceme nebo nechceme, bude pokulhávat za vývojem technologií ve světě. Osobní údaje vytvářejí ekonomickou hodnotu pro on-line platformy, jako jsou vyhledávače, sociální sítě, on-line videa apod. Analýzou osobních dat na internetu mohou internetové firmy lépe zacílit reklamy na své uživatele. Čím víc mají tyto firmy uživatelů a čím lépe umí personifikovat reklamy, tím mají větší zisk. Firmy jako Amazon, Meta Platforms (provozovatel Facebooku), Apple a Alphabet (provozovatel Googlu) mají z reklam roční tržby v řádu stovek miliard korun. Cílená reklama může pomoci i spotřebitelům. Slouží jako užitečný informační zdroj, protože je schopna zobrazit reklamy, které přímo souvisí s jejich zájmy. Poskytování osobních údajů tak může být výhodná jak pro on-line platformy, tak pro spotřebitele. Toto tvrzení platí v tom případě, kdy spotřebitelé mají důvěru v on-line platformy, že nevyužívají jejich osobní údaje k jiným účelům, než na jaké byla sjednána transakce. Pokud se docílí transparentního shromažďování osobních informací a spotřebitel je dostatečně chráněn zákonem (jako ten slabší), potom přínos z takových transakcí je pro obě strany.

Obecné nařízení o ochraně osobních údajů (GDPR) je tou ochranou spotřebitele před velkými firmami. Aby nedocházelo k jednostrannému využívání osobních údajů ze strany firem, ale aby spotřebitelé měli právo rozhodovat, jakým způsobem jejich osobní informace budou využívané. Jaké nové povinnosti pro zpracovatele osobních údajů GDPR zavádí?

- Povinnost vést záznamy o zpracování osobních údajů
- Posouzení vlivu na ochranu osobních údajů
- Ohlášení případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů
- Ustanovení pověřence pro ochranu osobních údajů

GDPR definuje také práva, které má osoba, poskytující osobní údaje. Subjekt údajů (občan, organizace, zaměstnanec) má:

- Právo na přístup ke svým osobním údajům
- Právo na opravu nepřesných údajů
- Právo na výmaz (právo být zapomenut)
- Právo na omezení zpracování, přenositelnost
- Právo vznést námitku proti zpracování osobních údajů
- Právo dodat stížnost u Úřadu pro ochranu osobních údajů (ÚOOÚ)

V rámci přípravy obecních úřadů na implementaci legislativy na ochranu osobních údajů, bylo třeba udělat několik opatření. Nejdříve ve veřejné sféře proběhla řada školení, aby se úřady mohly seznámit s tím, jaké povinnosti jim nově vzniknou. Poté obce začaly většinou spolupracovat s nějakou externí firmou, která využila příležitosti na trhu a začala nabízet implementaci GDPR na podmínky obecních úřadů. Nejdříve bylo potřeba udělat bezpečnostní audit. Tedy přehled toho, v jakém stavu je informační systém úřadu, a jaká má slabá místa. Poté následovala technická a organizační opatření.

3.2. Bezpečnostní audit

Obecní úřad má vlastní informační systém, který je součástí lokálního eGovernmentu. Informace uložené digitálně (data) mají jedinečnou hodnotu. Představme si situaci, že lokální počítačová síť byla napadena ransomwarem. K tomu mohlo dojít tak, že v obsahu nějakého mailu byl odkaz, na nějž někdo z úřadu bezmyšlenkovitě klikl. Pokud nebyla vnitřní síť dostatečně chráněna nebo byl antivirový program zastaralý, může dojít během

pár minut k zašifrování všech souborů v počítači, potažmo i na jiných místech v síti. Může dojít k totální ztrátě dat. Co by to pro obecní úřad znamenalo? Je dobré se projít touto představou, protože nás to motivuje k hledání lepších způsobů zabezpečení našeho informačního systému.

Než postoupíme k vytváření bezpečné informační sítě, musíme vědět, v jaké situaci se nacházíme a kam se chceme dostat. Bezpečnostní audit má odhalit slabá místa informačního systému. Bezpečnostní audit se vztahuje zpravidla na tyto oblasti:

- **Fyzická bezpečnost** – vztahuje se na všechny prostory, kde jsou jednotlivé prvky technické infrastruktury informačního systému. Může se jednat o kanceláře, nebo technickou místnost.
- **Technická infrastruktura** – zahrnuje všechny počítače, síťové prvky, server, router a napojení do veřejné sítě internetu.
- **Používaný aplikační software** – jsou všechny programy, které se využívají v rámci úřadu.
- **Poučená obsluha** – zaměstnanci pracující na svém počítači.

Když mluvíme o bezpečnosti, určíme si, co chceme chránit, co je naším aktivem. V našem případě to budou data (elektronické informace), která jsou využívaná v rámci úřadu. To, jakým způsobem a do jaké míry mohou být aktiva poškozena, vyjadřuje její zranitelnost (náchylnost k poškození). Na aktiva mohou působit různé hrozby (přírodního nebo lidského původu). Mohou pocházet zvenčí i zevnitř úřadu. Hrozby mohou být různého druhu: požár, krádež zařízení, chyba obsluhy, úmyslné poškození, kybernetický útok, porucha hardwaru. K prevenci vzniku škody provádí organizace opatření. Příklady opatření: lepší firewall proti kyberútoku, lepší fyzické zajištění technické místnosti, pořízení fotovoltaické elektrárny jako záložní zdroj elektrické energie atd.

3.3. SWOT analýza

SWOT analýza je další způsob vyhodnocení aktuální situace a zhodnocení rizik a příležitostí. Je to trochu jiný nástroj oproti bezpečnostnímu auditu. Má širší záběr, protože kromě rizik a slabých míst ukazuje i na silné stránky organizace. Příklad takové SWOT analýzy (analýzy silných a slabých míst, příležitostí a hrozeb) ukazuje tabulka níže. Silné a slabé stránky vycházejí z analýzy současného stavu. Příležitosti a hrozby ukazují

směr do budoucnosti. Hrozby ohrožují slabá místa naší organizace. Příležitosti znamenají použití silných stránek pro zamezení hrozeb.

Silné stránky	**Slabé stránky**
Zaměstnanec OÚ má znalosti ICT	Nedostatek financí na bezpečnost
Vysoká důvěra mezi pracovníky úřadu	Slabé fyzické zabezpečení
Kvalitní správce PC sítě	Absence dlouhodobé strategie rozvoje IS
Dobrá technologická infrastruktura IS	Zastaralý hardware
Podpora zastupitelů v bezpečnostní politice	Absence záložního zdroje
Příležitosti	**Hrozby**
Rozšířené využití elektronické spisové služby	Dlouhodobý výpadek elektrické sítě
Rozšířit a zabezpečit vnitřní WIFI pokrytí	Nedostatečná ochrana proti průniku škodlivého kódu
Výměna serveru za rychlejší a bezpečnější	Kyberútok, napadení ransomwarem
Sdílet zkušenosti s jinou obcí	Porucha hardware vedoucí ke ztrátě dat
Elektronizace poplatků za odvoz odpadu	Dlouhodobá nemoc správce sítě

Tabulka 1: Ukázka SWOT analýzy (vlastní zpracování)

3.4. Zabezpečení dat v lokální síti

Po provedení analýzy současného stavu, je třeba si také říct, kam se chceme jako úřad posunout. Již jsme si řekli, že aktivum, které chráníme, jsou data z našeho informačního systému. Data proto musí podléhat zvláštní ochraně. V podmínkách malých obcí se zabezpečení dat odvíjí od bezpečnosti informačního systému obce. Obecně lze říci, že data musíme chránit před zneužitím (způsobené například krádeží dat) a také před znehodnocením (ztráta dat, smazání dat, nedostupnost dat). Za příklad fatálního podcenění zabezpečení může sloužit instituce s názvem Národný bezpečnostný úrad Slovenskej republiky (NBU SR). V roce 2006 se skupině hackerů podařilo proniknout do e-mailového systému této organizace, která má bezpečnost přímo ve svém názvu. Nebylo to zvlášť obtížné, přihlašovací jméno bylo NBUSR a heslo NBUSR123.

Standard zabezpečení informačního systému malé obce

1) **Máme plán údržby a obnovy informačního systému úřadu.**

Není třeba mít dokonalé mnohastránkové směrnice o bezpečnosti, které nikdo nečte a nic z toho se nepoužívá. Každá vnitřní směrnice, pokud si ji úřad schválí, by měla být závazná. Stačí jednoduchý předpis toho, co je třeba v systému posílit (dokoupit, obnovit), popis odpovědností, systém zálohování dat, plán činnosti v případě napadení systému apod.

2) **Máme dostatečně zabezpečené fyzické prostory úřadu.**

Máte dobře zabezpečenou budovu obecního úřadu? Zvážili jste napojení na pult centrální ochrany (např. firma ANIM plus, Vsetín), kamerový systém, bezpečnostní dveře apod.? Jsou dveře do místnosti se serverem zamknuté a přístupné jen příslušné osobě? Máte přehled o pohybu osob na úřadě? Nezůstávají dveře do kanceláře otevřené, když v místnosti nikdo není? S technikou, kterou používáme (PC, notebook, mobil) zacházíme tak, aby se eliminovaly možnosti odcizení.

3) **Pravidelně zálohujeme a jednu zálohu uchováváme mimo budovu.**

V rámci zálohování je doporučeno řešit i uložení médií, na která se zálohování provádí. Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3-2-1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění informačního systému.

4) **Udržujeme software i operační systém aktuální.**

Správce systému musí pravidelně kontrolovat všechny prvky systému a zajistit jejich aktuálnost. Týká se to hlavně operačního systému a antivirového programu. Nesmí se také zapomenout ani na aktuální firmwary síťových prvků.

5) **Používáme antivirový program a firewall.**

Absolutní nezbytností je aktualizovaný antivirový program. Například produkt od firmy ESET Internet security dokáže kromě antivirové ochrany zajistit také dodatečnou ochranu. Chrání online platby a přístup do elektronického bankovnictví. Šifruje komunikaci mezi klávesnicí a prohlížečem, aby specifický

malware (keylogger) nemohl získat citlivá data typu hesel a podrobností o kreditních kartách. Funguje jako firewall. Brání neautorizovaným uživatelům v přístupu na zařízení a zneužití osobních dat. Upozorní uživatele na nevyžádané použití webové kamery. Umožňuje také otestovat domácí router a připojená chytrá zařízení na různé zranitelnosti. Odhalí podvodné internetové stránky, jež se snaží získat citlivá data, jako jsou uživatelská jména, hesla nebo bankovní údaje.

6) **Přihlašujeme se heslem do PC.**

I když si na úřadu důvěřujeme, měly by být počítače chráněny heslem. Je to z důvodu, že nevíme, kdo další může mít přístup k našemu PC. Při odchodu od počítače se ubezpečte, že jste se odhlásili. Svá hesla neuchovávejte na lístečcích nalepených na monitoru. Používejte pokud možno vícefaktorové autentizace do svých aplikací.

7) **Cizí paměťová media používáme na PC mimo lokální síť**

Cizí paměťové médium (nejčastěji USB flash disk) může být zavirované nebo obsahovat škodlivý kód. Antivir by měl tyto nástrahy zlikvidovat, přesto se na něj nemůžeme na 100 % spolehnout. Aby nedošlo k napadení počítačů v síti (jako třeba v případě ransomwaru) je doporučeno provádět operace s cizími médii na počítači, který není zapojen v síti (například notebook).

8) **Pravidelně školíme obsluhu počítačů.**

Pro všechny zaměstnance by měla být stanovena pravidelná školení týkající se základů kybernetické bezpečnosti a to minimálně 1× ročně. Při výskytu mimořádné události (např. nová obecně známá hrozba, zvýšený výskyt phishingových e-mailů apod.) je vhodné zorganizovat mimořádné školení, případně zaměstnance informovat jiným vhodným způsobem.

9) **Správce PC sítě má naši důvěru.**

Správce počítačové sítě dobře vybíráme. Pokud nemá dostatečnou kvalifikaci nebo mu nemůžeme důvěřovat, raději se poohlídneme po někom jiném. Správce sítě má největší vliv na to, jak je náš informační systém odolný. Má také přístup (hesla) do serveru a síťových prvků. To je, jako by měl obrazně klíče od obecního úřadu.

10) Máme informační systém zajištěn záložním zdrojem.

Bez elektrické energie není ani eGovernment. Obecní úřad by měl být vybaven záložním zdrojem pro případ dlouhodobého výpadku elektrické energie. Dobrým řešením může být fotovoltaická elektrárna se záložními bateriemi (lze pořídit i za pomocí dotace), která zároveň šetří náklady na provoz úřadu. Při současných cenách energií se náklady na pořízení fotovoltaické elektrárny vrátí řádově do několika let.

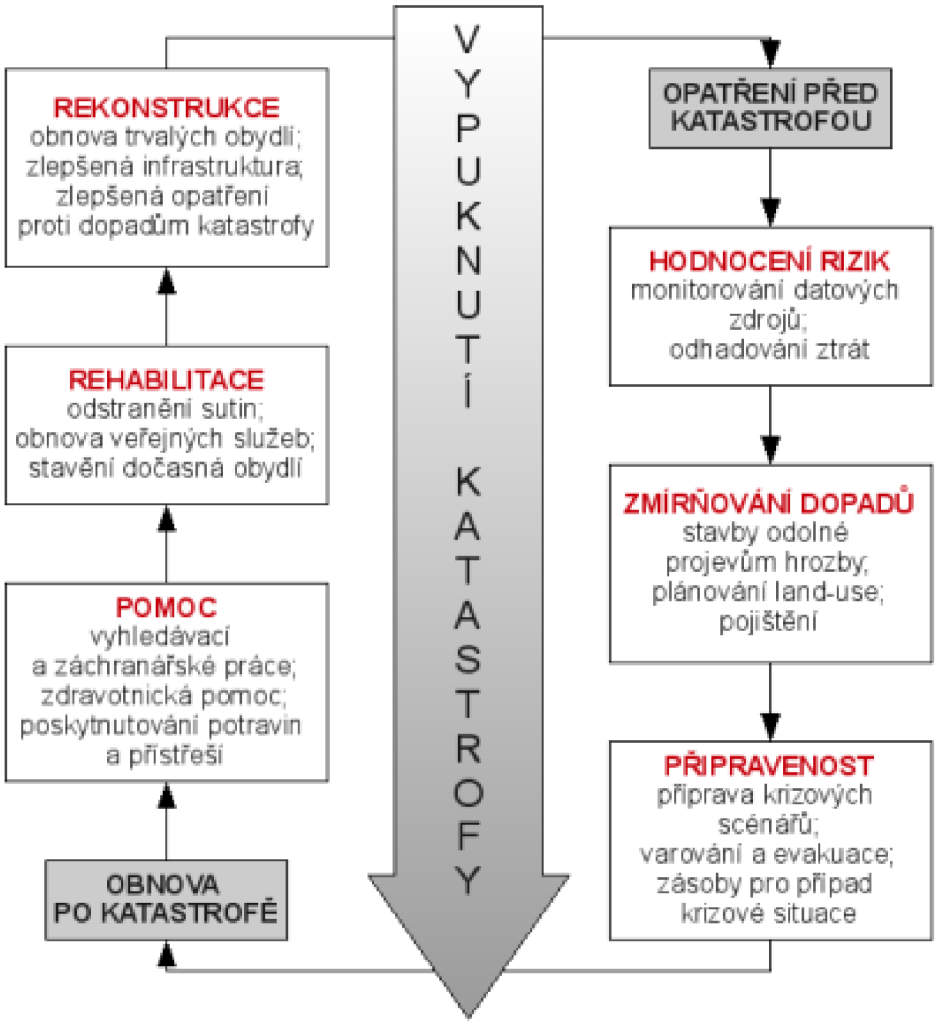
Kdo je připraven, není překvapen

Ekonomové říkají, že krize jsou nevyhnutelné. Otázkou není, jestli přijdou, ale kdy přijdou. Proto je dobré na informační systém místní správy hledět jako na nekončící proces vyhodnocování rizik, provádění preventivních opatření a řešení následků po incidentu. Obrazně se na tento koloběh můžeme dívat optikou zvládání přírodních katastrof. Před přírodní katastrofou (ale i před bezpečnostním incidentem) monitorujeme náš informační systém a zajišťujeme slabá místa proti možným hrozbám. Aktualizujeme firmware přístrojů, vyměňujeme zastaralé prvky komunikační infrastruktury, hardware i software udržujeme aktuální. Máme připravený rizikový plán, pro případ narušení systému. Pravidelně zálohujeme a kontrolujeme, zda jsou zálohy použitelné. V případě kybernetického napadení nebo jiného incidentu víme, koho máme přizvat k řešení problému. A pokud dojde k napadení systému nebo ke ztrátě dat, měli bychom mít stručný manuál, co v takovém případě dělat. „Obvykle se postupuje podle následujícího scénáře:

- Identifikovat, kde k bezpečnostnímu incidentu došlo
- Co nejvíce zamezit dalším škodám
- Analyzovat příčinu a zajistit stopy pro další analýzu
- Odstranit příčinu a obnovit funkčnost
- Zhodnotit škody
- Implementovat vhodná opatření k zamezení opakování incidentu

- Seznámit ostatní s výsledky šetření“[3]

V praxi bývá často zanedbaná analýza příčin, protože vedení organizace většinou požaduje rychlou obnovu provozu, a na zajištění důkazů a zjištění příčin tak nezbývá čas. Ignorováním analýzy příčin však velmi omezíme možnosti navržení a implementaci vhodných opatření pro zamezení opakování incidentu.



Obrázek 9: Koloběh bezpečnostních opatření, dostupné z [cit. 2022-03-16]: https://sites.google.com/site/teoretickavychodiska/predpoved_ochrana_obnova

[3] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. (s. 260)

Předcházení ztráty dat

Pokud máme zabezpečenou počítačovou síť podle standardu zabezpečení, můžeme se věnovat prevenci možných hrozeb. Na to existuje několik nástrojů. Nezmar (2019)[59] zmiňuje například systém prevence průniku (Intrusion Prevention Systém, zkratka IPS), který monitoruje síť na škodlivou činnost. Další nástroj je systém DLP (Data Loss Prevention). Rozlišujeme dva druhy DLP řešení. Síťová DLP pomáhají zabránit úniku citlivých dat na úrovni vnější komunikace společnosti. Endpoint DLP naproti tomu brání úniku dat z jednotlivých pracovních stanic společnosti. DLP systémy jsou významným pomocníkem především při ochraně před ztrátou dat způsobených vlastními zaměstnanci. DLP systémy jsou schopny efektivním způsobem zajistit odpovídající politiku přístupu k datům. K údajům pustí jen ty, kteří jsou oprávněni a zajistí využití dat pouze požadovaným způsobem. Do značné míry tak lze eliminovat selhání lidského faktoru. Nasazení DLP systému není všelék. Systém nedovolí uživateli data vytisknout nebo zkopírovat. Dá se to ale obejít tím, že údaje může uživatel vyfotit telefonem z obrazovky.

„Náklady spojené se ztrátou dat se liší dle odvětví. Ve službách hovoříme o nákladu ve výši cca 5000 Kč na záznam, ve světě financí pak o částce necelých 5,5 tisíc Kč a nejdražší jsou záznamy ve zdravotnictví, kde náklad na jeden řádek databáze vychází na téměř 8,5 tisíc Kč. Studie uvádí, že každá čtvrtá organizace se již s porušením integrity dat setkala. Studie mimo jiné ukazuje, že existuje přímá úměra mezi dobou, kdy dojde k odhalení porušení dat, a náklady s tím spojenými. Jednoduše platí, že čím později tím dražší.“ [4]

[4] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. (s. 264)

4. eGovernment rodinný a osobní

4.1. Jak si (ne)nechat ukrást peníze z bankovního účtu

Hackerské útoky nemusí cílit jen na naše data, ale v konečném důsledku i na naše bankovní účty. Přihlašovací údaje do internetového bankovnictví, údaje z platebních karet ani potvrzovací kódy z SMS zpráv žádná banka po svých klientech nikdy nepožaduje! A už vůbec ne po telefonu, v e-mailu, SMS zprávě nebo přes sociální sítě. Takovýto požadavek je pokusem o podvod, a proto na něj nereagujeme a informujeme banku. Je také dobré znát taktiku útočníků. Jaké nejčastější techniky tito moderní zloději používají? K popisu těchto technik můžeme využít informační platformy https://kybertest.cz/ a https://www.bezpecnebanky.cz/. Jsou to projekty České bankovní asociace společně s antivirovou společností ESET, Policií ČR a agenturou SC&C. Jak je uvedeno v úvodu: „Čím dál více využíváme moderních technologií – každý den brouzdáme po internetu, dostáváme a odpovídáme na emaily, pracujeme s internetovým bankovnictvím nebo nakupujeme v e-shopech. A přitom jsme často vystavováni hrozbám, které v případě naší nepozornosti či špatného rozhodnutí mohou vést ke ztrátě naší online identity či peněz z bankovního účtu.“[5]

Jaké jsou nejčastější typy útoků na klienty bank*?*

1. **Telefonáty podvodných bankéřů či policistů (vishing)**

Útočník vás chce vystrašit a zároveň vzbudit důvěru, že je tím, kdo vám pomůže ochránit peníze na účtu. Pod záminkou napadení vašeho účtu či podezřelé transakce vám zavolá v nezvyklý čas a představí se jako pracovník banky, či policista. Na hovor se dobře připraví – zná vaše jméno, adresu nebo číslo bankovního účtu. Může volat z čísla podobného či stejného, jako má vaše banka, dokonce vás vyzve k identifikaci, jako to dělají banky. S vaší získanou důvěrou vás pak bude tlačit k okamžitému převedení zůstatku na bezpečný účet, který je ale ve skutečnosti jeho. Scénáře se mohou lišit – útočník po vás bude chtít vaše přihlašovací údaje, údaje z vaší platební karty či potvrzovacích SMS, případně umožnit vzdálený přístup k vašemu PC. Závěr je ale stejný – své peníze již pravděpodobně nikdy neuvidíte.

[5] Kybertest, dostupné z https://kybertest.cz/projektu [cit. 2022-03-16]

2. Podvodné mobilní aplikace

Jedním z velmi aktuálních triků útočníků jsou i malwarem infikované mobilní aplikace či jejich aktualizace, které si nejčastěji stáhnete z neoficiálních obchodů s aplikacemi a webových stránek. Výjimkou ale nejsou ani podvodné aplikace nainstalované přímo z oficiálního obchodu. Pokud v telefonu nemáte nainstalovaný bezpečnostní software, který by vás varoval, a při instalaci aplikace udělíte vysoká oprávnění – například aplikaci pro nahrávání hovorů i přístup k fotoaparátu či SMS – dokáže odcizit vaše přihlašovací údaje do bankovnictví, obejít dvoufázové ověření či získat potvrzovací SMS zprávy. Aplikace proto nakupujte nejlépe jen na Google Play či App Store, čtěte jejich recenze a nedávejte jim více oprávnění, než potřebují.

3. Falešné stránky internetového bankovnictví

Jedná se již o známou útočnou metodu, přesto se může stát, že se díky své nepozornosti nachytáte. Útočník chce získat vaše přihlašovací údaje s pomocí falešné webové stránky banky. Ta může na první pohled vypadat úplně stejně jako skutečný web vaší banky, včetně loga a barev. Na druhý pohled ji ale odhalit lze – URL adresa webu se bude odchylovat od oficiálního názvu či zkratky banky, na stránce jsou překlepy, v řádku s adresou nebude visací zámeček označující bezpečnostní certifikát webu, nýbrž upozornění apod. Pokud se přes takové stránky přesto přihlásíte, získá útočník vaše přihlašovací údaje do internetového bankovnictví. Pomocí dalších podvodných technik mu pak stačí získat váš potvrzovací kód či autorizační SMS a cestu k vašim penězům na účtu má volnou.

4. E-maily plné virů a podvodných odkazů

V tomto případě jdou útočníci cestou kvantity nad kvalitou – rozešlou podvodné e-maily na mnoho adres včetně té vaší, kterou získali například z vašeho profilu na sociálních sítích, a čekají, kdo se chytne. Dávno už se nejedná jen o výzvy k převzetí dědictví po vaší zapomenuté tetičce či nabídky k sňatku od nigerijských princů, plné překlepů a gramatických chyb. E-maily se tváří jako oficiální zprávy banky, pošty nebo třeba obchodního řetězce. Obsahují odkazy na falešné stránky, kde máte zadat platbu či se přihlásit do internetového bankovnictví, případně vyzývají ke stažení přílohy, která je ale samozřejmě infikovaná virem či malwarem. Pokud trik včas neodhalíte, útočníci získají vaše přihlašovací údaje či údaje z platební karty.

5. Falešné profily na sociálních sítích

Útočníci typicky vytvoří falešný profil osoby, kterou znáte. Z tohoto profilu vás pak žádají o vyplnění formuláře či zaslání finanční částky na pomoc, případně pod záminkou výhry v soutěži posílají odkazy směřující na falešné stránky, kde již jen čekají, až zadáte vaše údaje z platební karty či jiné důvěrné údaje. Pokud podobnou výzvu obdržíte, raději si ji s danou osobou telefonicky ověřte. Podvodníci mohou ale falšovat i profilové stránky bank, přes ně se můžete dostat na falešné internetové bankovnictví či podvodnou platební bránu.

6. Získání nadvlády nad vaší platební kartou v mobilu

Získá-li útočník vaše údaje o platební kartě, pokusí se ji pravděpodobně tzv. digitalizovat, tedy ji nahrát do svého telefonu, resp. do Google Pay či Apple Pay. Pokud se mu následně podaří registraci potvrdit aktivačním kódem (zasílaným do internetového bankovnictví či SMS), ke kterému se dostane pomocí nějaké podvodné techniky, bude již moci "vesele" platit svým telefonem a odčerpávat vám peníze z účtu, dokud si toho nevšimnete.

Obrázek 10, zdroj NUKIB, https://www.nukib.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/ [cit. 2022-03-16]

4.2. Pět zásad pro bezpečí vašich údajů i vašich peněz

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovnictví ani čísla ze své platební karty. Banky se na ně opravdu NIKDY neptají, a to ani telefonicky, ani e-mailem, ani SMS či jinými zprávami. Zároveň nikdy neposílají odkazy na weby, kde jsou údaje vyžadovány!

2. Nereagujte na telefonní hovory, e-maily ani zprávy, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich záchranu. Kdyby byly vaše peníze skutečně v ohrožení, banka by již zareagovala dávno a bez vaší pomoci.

3. Nezadávejte ani v aplikaci nepotvrzujte platby, které vám někdo bude diktovat po telefonu. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.

4. Mějte aktualizovaný software a antivir v PC i telefonu. Aplikace stahujte jen z oficiálních zdrojů a nedávejte jim více oprávnění, než potřebují.

5. Buďte vždy v pozoru, nenechte se zviklat ani nalákat. V případě pochybností vždy kontaktujte svou banku či volejte policii (158).

5. Bezpečnostní opatření podle NUKIB

Další doporučení jsou na www stránkách NUKIB:
https://www.nukib.cz/cs/infoservis/doporuceni/ [cit. 2022-03-16]

Národní úřad pro kybernetickou a informační bezpečnost

ZÁKLADNÍ BEZPEČNOSTNÍ OPATŘENÍ PRO VRCHOLOVÉ VEDENÍ ORGANIZACE

Tento dokument je určen vrcholovému vedení organizací a čelným představitelům institucí – osobám, které mají největší vliv na směřování dané organizace a mají významné rozhodovací pravomoci. Důležitost těchto osob je však zároveň staví do pozice, kdy jsou lákavým cílem pro útočníky snažící se narušit kybernetickou bezpečnost organizace. Z tohoto důvodu je pro tyto osoby doporučeno dodržovat níže uvedená opatření ke snížení rizika ohrožení fungování organizace a naplňování povinnosti péče řádného hospodáře. Zároveň je potřeba mít vždy na paměti, že chování vrcholového vedení má odraz v chování běžných zaměstnanců – pokud vrcholové vedení pravidla nerespektuje, lze těžko vyžadovat plnění pravidel i po řadových zaměstnancích.

Tento dokument je doporučením a nenahrazuje žádné právní předpisy, tedy zejm. právní úpravu kybernetické bezpečnosti. Tento dokument nemůže nikdy pokrýt veškerá opatření, která lze aplikovat. Další opatření nad rámec tohoto dokumentu, vhodná pro danou organizaci, mohou navrhnout bezpečnostní specialisté v dané organizaci.

HLAVNÍ BEZPEČNOSTNÍ PRAVIDLO

RESPEKTOVAT BEZPEČNOSTNÍ POKYNY SPECIALISTŮ V DANÉ ORGANIZACI.
Každá organizace by se měla snažit dosahovat bezpečného prostředí a nakládání s daty. Za tímto účelem organizace také obvykle zaměstnává specialisty, kteří mají zabezpečení organizace na starosti. Jejich doporučeními, pokyny a návrhy je nutné se řídit a dodržovat je, jinak nemůže být bezpečnost nikdy na přijatelné úrovni. Neváhejte se na ně obrátit v případě dotazů nebo potřeby upřesnění těchto základních opatření.

PRÁCE S FIREMNÍM POČÍTAČEM NEBO SMARTPHONEM

NEPOUŽÍVAT SOUKROMÁ ZAŘÍZENÍ PRO PRACOVNÍ ÚČELY.
Soukromá zařízení nejsou pod správou organizace. S používáním soukromých zařízení je obvykle spojeno jejich neustálé přenášení, snížený dohled či sdílení se členy rodiny. Dále obsahují aplikace, které nejsou nutné k pracovním účelům. To vše přináší zvýšené riziko pro bezpečnost uživatele i celé organizace. Pokud jsou v organizaci soukromá zařízení přesto používána, obraťte se na bezpečnostní specialisty v organizaci a řiďte se jejich pokyny.

OMEZIT PŘÍSTUP K PRACOVNÍM ZAŘÍZENÍM A UZAMKNOUT JE POKAŽDÉ, KDYŽ JE POTŘEBA SE OD NICH VZDÁLIT.
Nehlídané zařízení dává prostor útočníkovi. Odemknuté zařízení bez dozoru dává komukoliv prostor k manipulaci s ním i jeho obsahem. To je potřeba mít na paměti nejen v kanceláři, ale především na veřejných místech (např. na konferenci, ve vlaku, apod.).

U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L.

U MAC počítače je nejjednodušší způsob rychlého zamknutí klávesová zkratka COMMAND + CONTROL + Q.

U mobilního zařízení stisknutí zamykacího tlačítka.

NEPŘIPOJOVAT NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Neznámá zařízení mohou obsahovat škodlivý kód, který se ihned po připojení dostane do zařízení. V případě nevyhnutelné nutnosti připojit neznámé médium je potřeba provést alespoň antivirovou kontrolu tohoto zařízení.

POUŽÍVAT HESLA, ČÍSELNÉ KÓDY NEBO JINÉ ZPŮSOBY ZABEZPEČENÍ TAK, JAK JE MÁ ORGANIZACE ZAVEDENÉ.
V případě ztráty nebo odcizení je zařízení podstatně lépe chráněno.

VOLIT DLOUHÉ, ZAPAMATOVATELNÉ FRÁZE PRO HESLA, PŘÍPADNĚ POUŽÍVAT SPRÁVCE HESEL.
Šifrovaný správce hesel umožňuje jednoduchou a bezpečnou správu všech potřebných přihlašovacích údajů a hesel na jednom místě.

PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ A HESEL SE UJISTIT, ŽE JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.
Především v případě pohybu na veřejném místě s větším počtem lidí, kamer nebo fotoaparátů (např. na konferenci, ve vlaku apod.), je zvýšené riziko, že útočník jednoduše zjistí a následně použije tyto údaje. V případě mobilních telefonů preferovat odemykání zařízení pomocí otisku prstu nebo skenu obličeje.

PROVÁDĚT AKTUALIZACI ZAŘÍZENÍ A NEVYPÍNAT PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU A PROGRAMŮ.
Aktualizace zařízení je způsob, jakým výrobce zařízení opravuje nově známé zranitelnosti, které by mohly toto zařízení ohrozit. Pokud má být aktualizace provedena, je potřeba jí nebránit a neodsouvat termín jejího provedení. Termín pravidelných automatických aktualizací je obvykle možno v zařízení nastavit. Stejně jako je tomu v případě aktualizací systému, také programy je potřeba aktualizovat. Program, který doposud fungoval bez problému, může být bez aktualizace téměř nepoužitelný a nebezpečný.

VYUŽÍVAT MOŽNOSTI ŠIFROVÁNÍ DAT NA INTERNÍCH I EXTERNÍCH ZAŘÍZENÍCH.
Šifrování zabezpečí data především při ztrátě nebo odcizení zařízení. Data na pracovním počítači by měla být šifrována, ale je nutno mít na paměti také ostatní zařízení, na kterých se tato data vyskytují.

PRAVIDELNĚ ZÁLOHOVAT DATA.
Vždy existuje riziko ztráty dat. Může se jednat o poruchu zařízení, jejich ztrátu nebo cílený útok, který data nenávratně zašifruje. Je proto vhodné myslet na zálohu důležitých dat a tuto zálohu uchovávat na jiném místě než v zařízení samotném, šifrovat a připojovat ji k zařízení pouze v okamžiku zálohování. Nezálohujte pracovní data na jiná než organizací určená zařízení.

VYVAROVAT SE POUŽITÍ VEŘEJNÉ WI-FI A DALŠÍCH VEŘEJNĚ NEBO ZDARMA POSKYTOVANÝCH SLUŽEB.
Veřejně poskytovaná Wi-Fi a další služby jsou jednoduchým způsobem, jak může útočník proniknout do zařízení a mít přehled o všech činnostech, především o použití přihlašovacích údajů a hesel. Problémem jsou zejména veřejné a nezabezpečené Wi-Fi (např. bez hesla, ale také s veřejně dostupným heslem – např. restaurace, konference apod.), a pokud to není nutné, je vhodné se k nim vůbec nepřipojovat. Tento problém je možné snížit použitím zabezpečeného spojení (tzv. VPN), nejvhodnější je pak používat VPN v kombinaci s mobilním internetem.

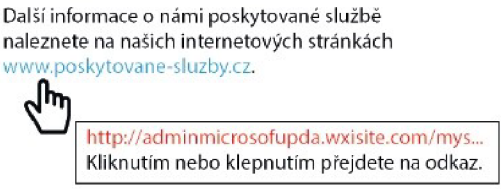
VĚNOVAT ZVÝŠENOU POZORNOST BEZDRÁTOVÝM TECHNOLOGIÍM, JAKO JE WI-FI, BLUETOOTH, NFC A DALŠÍ.
Bezdrátové technologie v zařízení je vhodné zapnout jen tehdy, pokud jsou využívány – představují potenciální cestu, jak proniknout do zařízení.

KONTROLOVAT, ZDA WEBOVÉ STRÁNKY PODPORUJÍ PROTOKOL HTTPS.
V případě internetových stránek, které vyžadují přihlášení (zejm. internetové bankovnictví, e-mail apod.), je potřeba věnovat pozornost, zda je taková stránka zabezpečena HTTPS protokolem. Pokud tomu tak není, nejsou zadané údaje vhodně zabezpečeny a jsou jednoduše zneužitelné.

Zobrazení HTTPS protokolu v internetovém prohlížeči

Zobrazení v internetovém prohlížeči bez protokolu HTTPS (přes tyto stránky nezadávat hesla)

NA INTERNETOVÉ ODKAZY KLIKAT OBEZŘETNĚ.
Je-li to možné, zkontrolovat, že odkaz nevede na podezřelou URL adresu. Skutečná URL adresa se po umístění kurzoru myši na odkaz bez rozkliknutí zobrazí vedle kurzoru (viz ilustrační obrázek), případně v okénku v levém dolním rohu stránky. Pokud nelze ověřit, kam odkaz vede, neklikat na něj.



SPRÁVNÁ A BEZPEČNÁ KOMUNIKACE

PŘISTUPOVAT K INFORMACÍM NA INTERNETU KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Je potřeba ověřovat, zda jsou informace skutečně pravdivé a zda jsou uvedeny v patřičném kontextu.

NEZVEŘEJŇOVAT OSOBNÍ ANI JINÉ CITLIVÉ INFORMACE.
Je potřeba zvážit, zda je skutečně nutné určité informace zveřejňovat. Data narození, náboženské vyznání nebo například fotografie mohou být následně zneužity, a to ať už proti konkrétním osobám, tak i proti organizaci, kterou tyto osoby zastupují.

OVĚŘIT IDENTITU PROTISTRANY PŘI KOMUNIKACI.
Je potřeba mít na paměti, že osoba, se kterou je komunikováno, se může vydávat za někoho jiného, což je zvláště důležité při prvotní komunikaci. Pokud existuje podezření, že osoba není tou, za kterou se vydává, je možné např. zavěsit a zavolat zpátky na telefonní číslo z oficiálního seznamu.

VĚNOVAT OBSAHU E-MAILŮ ZVÝŠENOU POZORNOST A V PŘÍPADĚ PODEZŘELÉHO E-MAILU NEBO PŘÍLOHY INFORMOVAT IT/BEZPEČNOSTNÍ ODDĚLENÍ ORGANIZACE.
Prostřednictvím příloh e-mailové zprávy se může jednoduše šířit škodlivý kód, který se po otevření přílohy aktivuje. Z tohoto důvodu je potřeba otevírat jen takové e-maily a jejich přílohy, které jsou důvěryhodné, a o těch podezřelých informovat IT oddělení.

CO JE TO PHISHING?
Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat uživatele na podvodnou stránku, nebo zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí. Neváhejte se obrátit na bezpečnostní specialisty v organizaci s dotazy, jak phishing poznat, případně využijte doporučení zveřejněná na stránkách NÚKIB, v sekci Infoservis – Doporučení – Spear-phishing a jak se před ním chránit.

NESDÍLET INFORMACE, KTERÉ JDOU NAD RÁMEC POTŘEBY AKTUÁLNÍ SITUACE.
Vše, co je obsahem komunikace, může být v budoucnu zneužito.

MÍT NA PAMĚTI, ŽE NIC NENÍ ZADARMO.
Nabídky a on-line služby zdarma, které jsou jindy placené, je potřeba důkladně zvažovat.

POKUD PROBÍHÁ KOMUNIKACE V ČASOVÉ TÍSNI, JE POTŘEBA O TO VÍCE UVAŽOVAT O JEJÍM OBSAHU A SDĚLOVÁNÍ POŽADOVANÝCH INFORMACÍ.
Útočníci rádi pracují s časovou tísní – teď je třeba něco vykonat, napravit, sdělit. Je potřeba to mít na paměti. Škoda z prodlení bývá menší než důsledky neuvážených činů.

ZABEZPEČENÍ ON-LINE ÚČTŮ

NEPOUŽÍVAT SOUKROMÉ ÚČTY PRO PRACOVNÍ ÚČELY A OBRÁCENĚ.
Soukromé účty (e-mailové schránky, cloudové služby, apod.) uživatele nejsou pod dohledem organizace a jsou tak pro organizaci zvýšeným rizikem např. z důvodu zvýšeného rizika infikování firemní sítě škodlivým kódem. Platí to i obráceně; pracovní účty není žádoucí používat pro soukromé účely.

PŘÍSTUPY K PRACOVNÍM ÚČTŮM CHRÁNIT HESLY. PRO KAŽDOU SLUŽBU POUŽÍVAT JINÉ UNIKÁTNÍ HESLO.
V případě používání slabého hesla je jeho prolomení útočníkem otázkou okamžiku. Pokud dojde k vyzrazení hesla k jednomu účtu, má útočník možnost použít stejné heslo i u jiných účtů.

NESDĚLOVAT JINÝM OSOBÁM PŘIHLAŠOVACÍ ÚDAJE A HESLA K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu nebo hesla do počítače může mít takové jednání závažné následky.

V PŘÍPADĚ, ŽE JE TO MOŽNÉ, VYUŽÍVAT VÍCEFAKTOROVOU AUTENTIZACI, A TO PŘEDEVŠÍM U SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL A DALŠÍ.
Běžným způsobem realizace vícefaktorové autentizace je obdržení kontrolní SMS po zadání přístupových údajů. V organizaci však mohou existovat i jiné způsoby vícefaktorové autentizace uživatelů.

PRO BĚŽNOU ČINNOST VYUŽÍVAT BĚŽNÝ UŽIVATELSKÝ ÚČET. ADMINISTRÁTORSKÝ ÚČET JE URČEN PRO TY, KDO VYKONÁVAJÍ SPRÁVU SYSTÉMŮ A ZAŘÍZENÍ V ORGANIZACI.
Administrátorský účet s vyššími oprávněními je určen výhradně pro správu systému, typicky prostřednictvím IT oddělení.

NEPOUŽÍVAT KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nikdy není vhodnou alternativou k obnovení hesla zadávat kontrolní otázky typu „nejmenší planeta sluneční soustavy" či „rodné jméno manželky". Podobné informace jsou či mohou být dohledatelné z veřejných zdrojů. Je-li taková kontrolní otázka povinná, je potřeba k ní přistupovat jako k heslu a volit ji tak, aby nebyla dohledatelná.