Sborník
konference

ISSS 2023

25. ročník konference

15.–16.5.23
HradecKrálové

CALENDARIUM REGINA

S podporou města Hradec Králové

generální partner

hlavní partneři

partneři

Vydáno u příležitosti **25. ročníku konference** ISSS

Záštitu konferenci poskytli

Miloš Vystrčil, předseda Senátu Parlamentu České republiky
Petr Fiala, předseda vlády České republiky
Vít Rakušan, 1. místopředseda vlády a ministr vnitra
Ivan Bartoš, místopředseda vlády ČR pro digitalizaci a ministr pro místní rozvoj
Martin Kupka, ministr dopravy
Asociace krajů České republiky

Obsah

Digitalizace procesu sběru a správy dat spotřeb energií v organizacích Královéhradeckého kraje

Ing. Lenka Bacovská, vedoucí oddělení projektového řízení CIRI
Ing. Bořek Dvořáček, referent pro energetiku KÚ KHK

Projekt Rozvoj systému hospodaření s energií v Královéhradeckém kraji

Projekt *Rozvoj systému hospodaření s energií v Královéhradeckém kraji (KHK)* je dalším kvalitativním krokem v zavedeném systému managementu hospodaření s energií v KHK. Královéhradecký kraj má již od roku 2018 zaveden a certifikován systém managementu hospodaření s energií (dále také „EnMS"), který specifikuje základní nástroje, metody a postupy, které se uplatňují při řízení energetické hospodárnosti objektů v majetku Královéhradeckého kraje a je držitelem certifikátu dle ČSN EN ISO 50001:2012, resp. ČSN EN ISO 50001:2019.

V certifikovaném systému je zahrnut sám kraj a jeho 100 organizací (v průběhu času dochází ke změnám v rámci jednotek případů; nejsou zapojeny organizace, které sídlí v pronajatých prostorách). Povinnosti pro zapojené organizace vyplývající z nastaveného systému jsou popsané ve Směrnici č. 27 upravující Systém managementu hospodaření s energií v organizacích Královéhradeckého kraje, kterou schválila Rada Královéhradeckého kraje. Nejužší tým EnMS je tvořen představitelem vedení kraje (PVK; 1 osoba), energetikem kraje (EK; 1 osoba), interním auditorem (IA; 1 osoba), odbornými konzultanty pro energetiku (OKE; 3 osoby), dále jsou v týmu představitelé vedení organizací (PVO; 100 osob) a energetičtí manažeři organizací (EMO; 100 osob).

Pilířem projektu *Rozvoj systému hospodaření s energií v Královéhradeckém kraji*, je **zavedení systému dálkových odečtů spotřeb jednotlivých druhů energií a médií** (elektřina, plyn, teplo, voda). Dříve používaný systém pro evidenci dat byl uživatelsky nepřívětivý s minimálními funkcemi, byl pořízen v roce 2012 a od té doby nebyl aktualizován ve smyslu funkčních či uživatelských nároků.

Královéhradecký kraj se rozhodl, mimo jiné, i na základě podnětů od jednotlivých organizací, k **zavedení systému dálkových odečtů spotřeb jednotlivých druhů energií a médií**.

Dalšími aktivitami projektu *Rozvoj systému hospodaření s energií v Královéhradeckém kraji* je vytvoření **elektronického modulu kalendáře revizí** a vytvoření **modulu e-learningového vzdělávání týmu EnMS**.

Prvním krokem v rámci přípravy realizace výše uvedených aktivit byla inventarizace měřidel, kterou provedli členové týmu EnMS. Inventarizace proběhla formou osobních návštěv jednotlivých budov, kde byla zhotovena fotodokumentace umístění měřidel, dále byla vytvořena mapka s vyznačením umístění měřidel v budovách, proveden soupis kódů jednotlivých měřidel (EAN, EIC), velikost jističů, typ měření. Tyto informace byly podkladem pro výběr dodavatele systému dálkových odečtů. Požadavkem na systém byla dále funkce kalendáře revizí a e-learningu, tak aby bylo vše k dispozici v jednom systému.

Poř.č.	Typ měřidla	Dálkový odečet	Jistič	Dodavatel	Fotodokumentace	poloha	Poznámka
1.	Elektroměr NN	ANO	3x160A	Pražská plynárenská	ANO	přízemí	
2.	Plynoměr VO	ANO		Pražská plynárenská	ANO	přízemí	
3.	Plynoměr MO			Pražská plynárenská	ANO	suterén	
4.	Vodoměr "suterén"			VAK Náchod	ANO	suterén	
5.	Vodoměr "F"			VAK Náchod	ANO	přízemí	

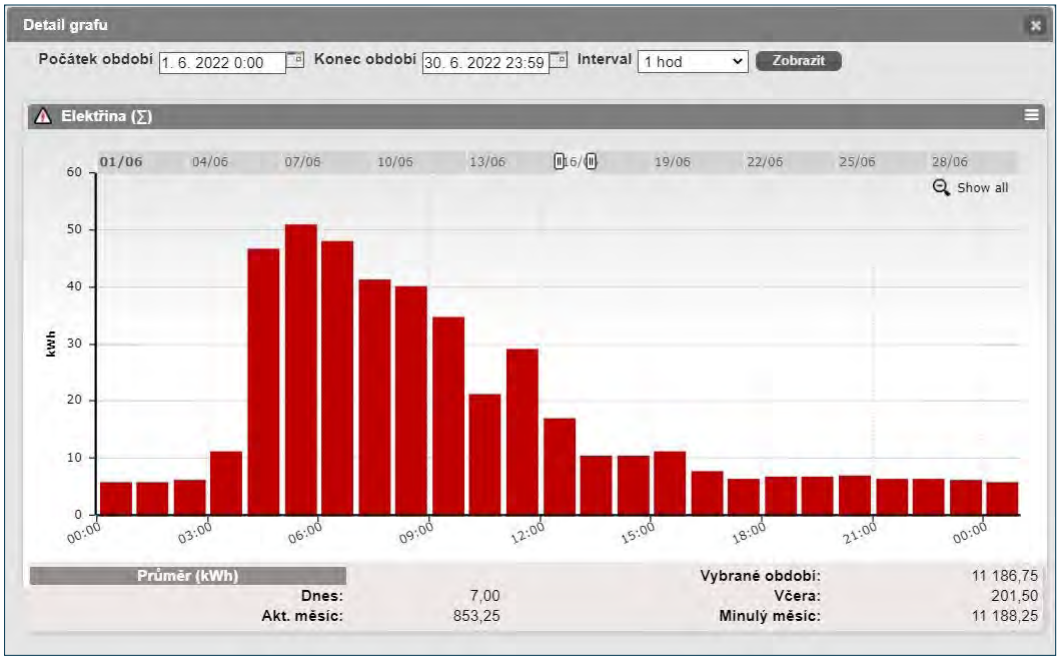
Základní funkce systému

- řízení přístupových práv jednotlivých uživatelů kombinací práv vyplývajících z uživatelských rolí (jaké typy dat lze prohlížet/editovat) a práv k datům z nastavených objektů (ze kterých objektů lze data číst/editovat),
- dálkové odečítání měřičů spotřeby a čidel,
- ukládání a archivace odečtených dat,
- on-line a off-line analýzy dat (grafy, tabulky, reporty...),
- on-line monitoring (události a alarmy),
- obchodní podporu (reporty, přehledy...),
- řízený přístup k systému přes WEBové rozhraní přes veřejný Internet (WEBový portál).

Analytický modul

umožňuje nastavení konfigurovatelných grafů, které poskytují tyto možnosti:

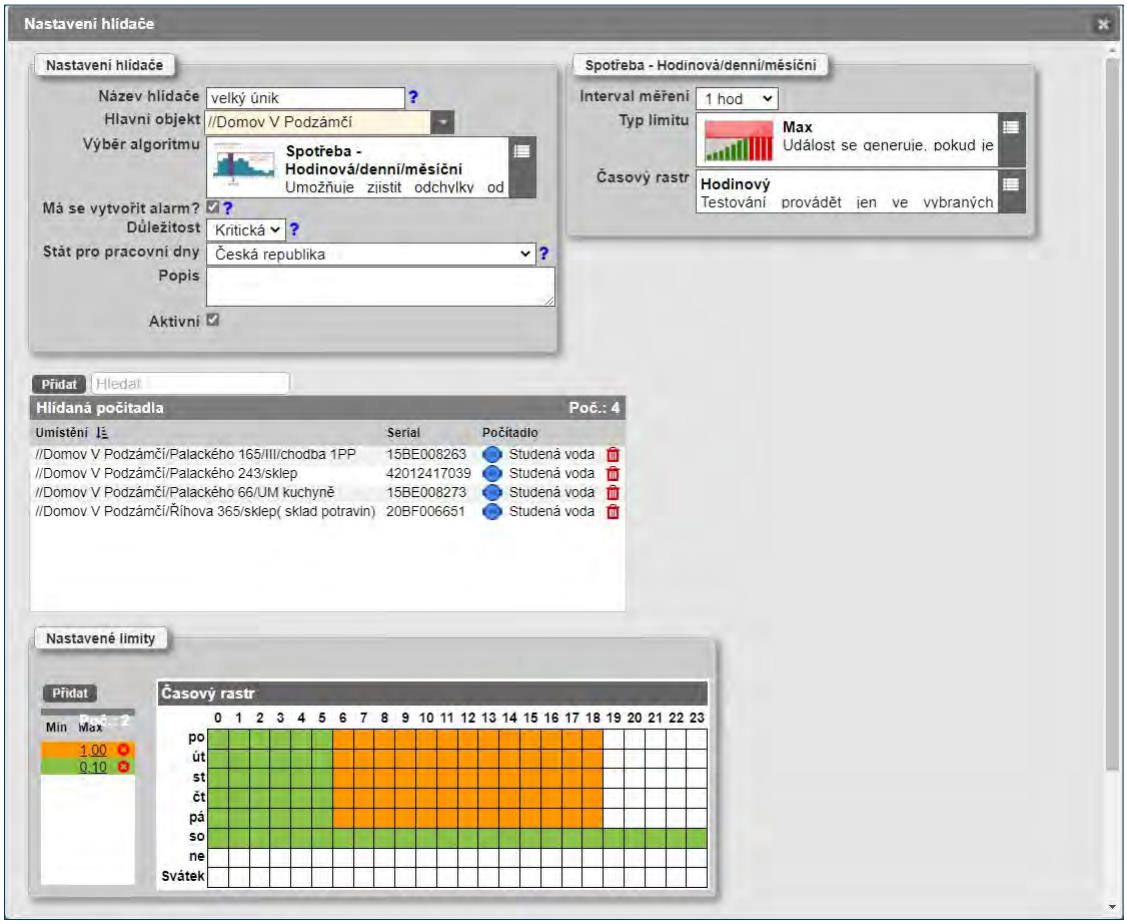
- interpretaci dat po různých časových úsecích („obdobích“ a „granulích“) s možností prokládání historickými daty (srovnání s předchozím obdobím, meziroční srovnání), nebo s referenčními daty;
- možnost srovnání výsledků analýz z více objektů ve stejném časovém úseku
- zobrazení dat ve vícevrstvých grafech ve formě sloupcových, čárových, bodových, skládaných sloupcových a koláčových grafů.



Události a alarmy

Součástí monitorovacích funkcí systému je **subsystém generování alarmů**, které slouží pro odhalení změn ve spotřebě, které signalizují úniky nebo havárie vody/plynu apod. Každou hodinu vyhodnocuje systém spotřebu za uplynulých „X“ hodin („délka intervalu“). Pokud spotřeba za nastavenou délku intervalu překročí (v součtu) zadaný limit, systém okamžitě odesílá informaci uživateli objektu (případně dalším dle nastavených kontaktů) o nadměrné spotřebě energie/média. Alarmy lze nastavit v několika algoritmech.

Celkem se jedná o 1 071 odběrných míst sledovaných dálkově ve 100 organizacích na 275 lokacích (adresách).



Modul „kalendář revizí“

Je součástí nově zavedeného systému, slouží pro podporu provozu objektů a umožňuje plánovat a vyhodnocovat jednorázové i periodické úkoly (např. opravy, **revize, kontroly**) na měřidla a na ostatní zařízení.

Modul e-learningu

Je také součástí nově zavedeného systému má dvě části, edukační a testovou. Členům týmu EnMS poskytuje studijní materiály, jak ve formě souborů ke stažení, tak umožňuje prohlížení materiálů přímo ve webovém rozhraní. Systém umožňuje nastavit povinnost postupného prohlížení jednotlivých vzdělávacích částí. Další funkcí tohoto modulu je testová část, kde je možné nastavit počet otázek, které musí být zodpovězeny správně, aby člen týmu EnMS úspěšně absolvoval proškolení, čas na zpracování a odeslání výsledků testu. Uživatel je ihned informován o výsledku testu. Současně Královéhradecký kraj má on-line přehled stavu proškolení členů týmu EnMS (jmenný seznam s datem provedení a výsledkem testu), které musí být dle normy ČSN EN ISO 50001:2019 průběžné a doložitelné při re/certifikačním auditu.

Příručka pro energetické manažery organizací Královéhradeckého kraje

Jako další vzdělávací materiál byla vytvořena publikace obsahující základní pojmy a pravidla v energetice. Vzhledem k rozsahu tématu pochopitelně nemůže příručka pojednávat o oboru energetika v celé jeho šíři a hloubce. Může však posloužit všem, kteří se chtějí blíže seznámit se principy v energetice.

Použité technologie

Hlavní způsob získání dat o spotřebě energií a médií z jednotlivých měřidel zvoleného řešení je sběr dat prostřednictvím bezdrátových modulů. V případě menší koncentrace měřidel v dané lokalitě (cca do 15 měřidel), jsou použity rádiové moduly NB-IoT s odpovídajícím datovým rozhraním, které zajišťují přenos dat bezdrátově na nejbližší základnovou stanici mobilního operátora a dále prostřednictvím jeho datové sítě. V případě větší kumulace měřidel je využita bezdrátová síť v pásmu 169 MHz (zřízení potřebného počtu základnových stanic 169 MHz na vybraných objektech. Sběr dat z měřidel na tuto základnovou stanici probíhá v pásmu 169 MHz, ze základnové stanice pak v pásmu GSM.) Tam, kde jsou využívány rádiové moduly v pásmu 868 MHz nebo 433 MHz, jsou použity převodníky 868/433 MHz na NB-IoT nebo 169 MHz. Předností je vzájemná kompatibilita různých zařízení od různých výrobců.

Ukazatele dosažení cílů

1. Zrealizovaná digitalizace sběru dat spotřeb energií Královéhradeckého kraje a jeho organizací zapojených v EnMS
2. Počet dálkově odečítaných měřidel energií (celkem 1 071 ks):
   i. Kalorimetry 108 ks odečet každou 1 hodinu
   ii. Elektroměry 437 ks odečet každou ¼ hodinu
   iii. Plynoměry 225 ks odečet každou 1 hodinu
   iv. Vodoměry 301 ks odečet každou ¼ hodinu (online)
3. Snížení počtu pojistných událostí, resp. minimalizace škod
4. Relevantní data pro vyhodnocení systému energetického managementu za kalendářní rok
5. Zajištění možnosti sjednocení evidence revizí a kontrol elektronickou formou v KHK
6. Zavedení možnosti vzdělávání členů týmu EnMS formou e-learningu
7. Zajištění průkazného přehledu vzdělávání členů týmu EnMS

Zainteresované strany

Za Královéhradecký kraj byl realizací pověřen nejužší tým EnMS, který je tvořen představitelem vedení kraje, energetikem kraje, interním auditorem a odbornými konzultanty pro energetiku z Centra investic, rozvoje a inovací, která je příspěvkovou organizací Královéhradeckého kraje (dále také „CIRI“). Projekt dálkových odečtů by nebylo možné realizovat bez úzké spolupráce s představiteli vedení organizací a energetickými manažery jednotlivých organizací. Zejména fyzická inventarizace měřidel vyžadovala spolupráci a součinnost energetického týmu s vedením a energetickými manažery organizací. Dalšími organizacemi, které se podílely na řešení, byly dodavatelé energií. Byla navázána spolupráce s distribučními společnostmi, které dodávají jednotlivé druhy energií a médií. Tam kde dodavatelé již uskutečňovali své dálkové odečty spotřeb energií, např. u elektrické energie společnost ČEZ Distribuce u typu měření „A“ a „B“, je dohodnut import dat z portálu naměřených hodnot PND, stejným způsobem byla zahájena spolupráce se společností GasNet pro import dat spotřeb plynu z portálu AVE. Obě společnosti jsou výhradními distributory těchto energií v celém Královéhradeckém kraji. Složitější situace je u dodavatelů tepla a vody. Jedná se o lokální dodavatele, ale se všemi se podařilo najít v této problematice shodu. Všechny dodavatelské organizace spolupracovaly nad

rámec povinností a ty menší využily projektu ke zvýšení povědomí o inovacích v oboru. Vzhledem k velkému počtu zainteresovaných subjektů je patrné, že bez úspěšného vyjednávání, součinnosti a vzájemné úzké týmové spolupráce by tak inovativního a efektivního řešení nemohlo být dosaženo.

Doporučení pro implementaci v další organizaci

Celý projekt je nadčasovým a inovativním řešením systému hospodaření s energií ve veřejné správě. Inovativnost spočívá v digitalizaci procesů orgánu veřejné správy v oblasti energetického hospodářství s jednoznačně pozitivním vlivem na zaměstnance kraje a jím zřízené a ovládané organizace. Prostřednictvím tohoto inovativního procesu dochází k zajištění jednotného a porovnatelného přehledu spotřeb jednotlivých druhů energií a médií na jednotlivých organizacích kraje v čase. Slouží k celkovému vyhodnocení efektivnosti procesu nastavení energeticky úsporných opatření a kladení důrazu na energetickou hospodárnost, vyžadovanou od představitelů organizací. Je to inovativní proces nejen pro vedení veřejného subjektu, ale i pro jeho zaměstnance svým nadčasovým řešením a uvedenými prvky novosti, které motivují tyto pracovníky k jejich dalšímu pozitivnímu rozvoji v rámci svého pracovního působení. K předání zkušeností a sdílení know-how jsme již byli ze strany jiných veřejných subjektů osloveni a probíhá proces sdílení dobré praxe.

Analýza stavu konektivity v České republice s bližším zaměřením na obce

Ing. Lucie Burianová, Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra regionálních studií

Úvod

Digitální technologie hrají stále signifikantnější roli v otázce rozvoje ekonomik [1]. Růst investic do ICT koreluje s pozitivním efektem na ekonomický růst a produktivitu [2]. Vzhledem k trendům souvisejících s digitální transformací v podobě např. umělé inteligence, Internet věcí či Big data je pro optimální a efektivní užívání nutná odpovídající softwarová i hardwarová infrastruktura. Jednou ze zcela základních komponent pro digitální transformaci je internetového připojení. Kvalitní a rychlé internetové připojení je jednou z klíčových komponent pro rozvoj podnikání, zvyšování produktivity a zlepšování kvality života obyvatel a zvyšování konkurenceschopnosti. Důraz na dostupnost internetového připojení byl řešen již na konci 20. století [3]. Některé studie prokazují, že existence internetové připojení snižuje chudobu venkovských oblastí, a to zejména díky benefitu v podobě zvyšování produktivity. Společně s vývojem digitálních technologií se zároveň zvyšují požadavky na jeho rychlost.

Evropská unie každoročně provádí analýzu vývoje digitalizace členských států pomocí Indexu digitální ekonomiky a společnosti (DESI) [4]. Součástí je klíčová oblast konektivita, která monitoruje metriky spojené s internetovým připojením. V rámci této kategorie vykazuje Česká republika výsledky, které jsou dlouhodobě pod průměrem EU. ČR se snaží prostřednictvím programů a iniciativ souvisejících s budováním digitální infrastruktury v oblasti konektivity specifické problémy řešit. V reakci na problematické oblasti týkající se konektivity byl v roce 2021 schválen Národní plán rozvoje sítí s velmi vysokou kapacitou. Dokument definuje strategický postup při výstavbě sítí, u kterých by měla být podpora směřována z veřejných zdrojů. MPO pravidelně vypisuje výzvy na vybudování vysokorychlostních sítí ve špatně přístupných lokalitách. I přesto se stále nedaří oslovit cílené žadatele a problematiku bílých míst efektivně vyřešit.

Analýza prostředí vysokorychlostního připojení v ČR se zaměřením na obce

Česká republika dlouhodobě vynakládá značné prostředky na podporu digitální ekonomiky a rozvoj digitální infrastruktury. V roce 2021 bylo do ICT a software vynaloženo 298,9 miliardy Kč [5]. Tyto investice zahrnují i podporu konektivity. Jmenovitě se jedná o rozšíření širokopásmového internetu, pokrytí mobilních sítí, výstavbu datových center a další potřebnou infrastrukturu podporující digitalizaci a digitální transformaci ČR.

Na podporu konektivity byla přijata řada programů a iniciativ. Konkrétně se jedná např. o Operační program Podnikání a inovace pro konkurenceschopnost (OP PIK), který poskytuje finanční podporu k rozvoji digitální infrastruktury a technologií pro podnikání. Přičemž jednou z podporovaných oblastí je zvyšování rychlosti a pokrytí širokopásmovým připojením. Dalším příkladem je Strategie digitální ekonomiky, ve které byla přijata opatření pro rozvoj digitální infrastruktury se zaměřením na zlepšení připojení na venkovských oblastech. Podpoře venkova se věnuje i Program digitalizace venkova, který nabízí finanční podporu na zlepšení přístupu internetu. Konektivita je řešena i v projektu Digitální Česko, který si klade za cíl poskytnout kvalitní a rychlé připojení k internetu pro všechny obyvatele ČR.

Pokud bychom se zaměřili na konkrétní ukazatele, tak Česká republika se v Indexu DESI 2022 v kategorii konektivity umístila na 17. místě [6]. Zároveň se jedná o oblast, ve které byla hodnocena nejhůře. V následující tabulce, která komparuje vybrané indikátory kategorie konektivity v čase si lze povšimnout nejvýznamnějších dlouhodobých problémů, které se prozatím nedaří účinně řešit. Index DESI ukazuje vždy čísla, která jsou v dané zemi sesbírána za předchozí rok.

Tab. č. 1: Vývoj konektivity v ČR

Rok	2022	2022	2021	2021	2020	2020	2019	2019	2018	2018
Pořadí	17		22		24		19		19	
	ČR	EU	ČR	EU	ČR	EU	ČR	EU	ČR	EU
Využití pevného širokopásmového připojení	84 %	78 %	83 %	77 %	74 %	78 %	74 %	77 %	73 %	75 %
Využití pevného širokopásmového připojení s rychlostí alespoň 100 Mb/s	27 %	41 %	24 %	34 %	20 %	26 %	18 %	-	-	-
Využití připojení s rychlostí alespoň 1 Gb/s	0,77 %	7,58 %	0,37 %	1,30 %	<0,01 %	-	-		-	-
Pokrytí NGA	93 %	90 %	97 %	87 %	92 %	86 %	90 %	83 %	89 %	80 %
Pokrytí VHCN	52 %	70 %	33 %	59 %	29 %	44 %	21 %		-	-
Pokrytí optickou sítí (FTTP)	36 %	-	33 %	-	29 %	-	-	-	-	-
Pokrytí sítěmi 5G	49 %	66 %	0 %	14 %	-		-	-	-	-
Index cen širokopásmového připojení	67	73	59	69	57	64	88	87	87	87

Vlastní zpracování podle EU Index Desi

Česká republika disponuje nedostatečným počtem domácností využívajících pevné širokopásmové připojení s rychlostí 100Mb/s a zároveň je zde zanedbatelné procento, které využívá připojení s rychlostí alespoň 1Gb/s. U obou ukazatelů se diference od průměru EU stále více prohlubuje.

Významně pod průměrem EU je ČR i v pokrytí VHCN, sítěmi s velmi vysokou kapacitou, a poté v pokrytí optickou sítí FTTP. Pokrytí sítěmi s velmi vysokou kapacitou je řešeno ze strany vlády i soukromých společností. V rámci řešení problematiky VHCN byl schválen Národní plán rozvoje sítí s velmi vysokou kapacitou, který reflektuje jejich důležitost. Nicméně je patrné, že se stav pokrytí VHCN meziročně zvýšil, což nastalo z důvodu zavádění technologie Doscis 3.1. Soukromé společnosti, příkladem CETIN, O2 či Vodafone, taktéž investují do výstavby VHCN sítí za účelem poskytnutí vyšší rychlosti internetového připojení pro své zákazníky.

Na pokrytí optickou sítí FTTP existuje v ČR několik programů a iniciativ. V roce 2019 byl přijat Národní plán rozvoje optických sítí, který si klade za cíl do roku 2025 pokrýt optickými sítěmi nejméně 95% obyvatel. V plánu je iniciováno na podporu pokrytí sítěmi ve venkovských oblastech, kde je výstavba nákladnější a problematičtější. Podpora výstavy optických sítí je řešena i soukromými subjekty, tedy poskytovateli internetových služeb, jako je např. O2 či Vodafone. Tyto firmy investují do výstavby optických sítí v rámci vlastních programů ke zlepšení dostupnosti a rychlosti internetového připojení pro zákazníky.

V roce 2021 činil meziroční nárůst pokrytí 5G sítěmi 49 %, což je taktéž výsledek pod průměrem EU. Problematice 5G sítí je podrobněji věnována následující kapitola.

Vybrané specifické problémy ČR v oblasti konektivity

V České republice se dlouhodobě projevují problémy vysokých cen mobilních sítí, oproti jiným státům EU. A poté kontroverze výzev MPO na podporu konektivity, které nejsou schopné adekvátně cílit na žadatele. Následující kapitola je věnována těmto specifickým problémům.

Síť 5G představuje telekomunikační standard nové mobilní sítě. Na rozdíl od svých předchůdců odpovídá vyšším standardům při komunikaci a zároveň splňuje požadavky pro komponenty vztahující se k trendu Průmyslu 4.0. Česká republika zaostává u pokrytí 5G sítěmi. V současné době je pokryto 49 % z osídlených oblastí, přičemž průměr EU je 66 %. Nicméně, report z EU také uvádí, že pokrytí 5G sítěmi u venkovských oblastí je 43,3 % a v EU je průměr 34,7 % [6]. Problémy, které jsou spojené s konektivitou v rámci 5G sítě je vysoká cena a nedostatečné pokrytí.

Jedním z hlavních problémů je nedostatečná konkurence v oblasti telekomunikací. Tržní podíl třech největších poskytovatelů mobilních služeb (T-Mobile Czech Republic a.s. s 38,8 %, O2 Czech Republic a.s. s 28,8 % a Vodafone Czech Republic a.s. s 25,1 %) v roce 2021 přestavoval přes 91 % celkového trhu [7], což může negativně ovlivnit dopad na koncového zákazníka.

Ceny mobilních dat, kam spadá i využívání 5G sítě, jsou jedny z nejvyšších v Evropské Unii. Při porovnání balíčku, který obsahuje 5GB dat a 300 hovorů, zaplatí zákazník v České republice 35,63 eur měsíčně. Za stejný produkt zaplatí obyvatel Dánska 16,1 eura, obyvatel Nizozemska 13,68, přičemž mají uživatele v těchto zemích mnohem lepší úroveň pokrytí než v ČR. Dále v Polsku obyvatelé zaplatí 9 eur, v Rakousku 8,74 eur a na Slovensku 25,36 eur, přičemž průměr EU je pro tento objem dat 16,4 eur [8]. (Všechny uvedené ceny jsou přepočteny na paritu kupní síly). Trend vyšších ceny mobilních v rámci Evropské unie i celé Evropy jsou patrné i pro ostatní balíčky – produkty s různými objemy dat.

Další problémem 5G sítí je nedostatečné pokrytí území v ČR. V roce 2021 dosahovalo pokrytí území sítěmi 5G téměř 30 %, kde největší podíl měl Vodafone s cca 21 %, poté T-mobile s 10 % a nejméně bylo pokryto společností O2 a to kolem 3 %. Lepší situace byla v roce 2021 v oblasti pokrytí obyvatelstva sítěmi 5G, když celkově bylo pokryto obyvatelstvo z téměř 70 %. Podstatně největší zastoupení měla společnost Vodafone s celkovým pokrytím přes 60 %, dále T-mobile se zhruba 35 % a poslední opět O2 s pouhými cca 4 % [9].

V České republice proběhla v roce 2020 aukce kmitočtu pro 5G sítě. Klíčové aukční bloky získaly stávající velké firmy na trhu: T-mobile, Vodafone a O2, které zároveň získalo blok se závazkem národního roamingu. Noví hráči, Nordic Telecom a Centronet, získali pouze dílčí bloky u méně klíčových kmitočtů a jsou tedy závislí na O2. Tato aukce byla klíčová z důvodu možného řešení dlouhodobého problému s vysokými ceny dat. Očekával se vstup čtvrtého významného hráče, díky kterému by se ceny podařilo regulovat.

Ministerstvo průmyslu a obchodu iniciuje výzvy na podporu výstavby sítí pro vysokorychlostní internet v ČR. V rámci OP Podnikání a inovace v programovacím období 2014–2020 byla vyhlášena I. výzva programu podpory Vysokorychlostní internet. Cílem výzvy bylo podpořit výstavbu sítí s minimální rychlostí 30 Mb/s do lokalit, ve kterých nebyl přístup doposud zajištěn. Tato výzva skončila fiaskem a z původně vyčleněných 11 miliard bylo nakonec zažádáno o 47 milionů Kč. Dotační program byl určen pro 81 intervenčních míst, tedy bílá místa, kde se nachází necelých 5% obyvatel. Tato místa obvykle pro podnikatelské subjekty nebývají atraktivní a současně s vysokou administrativní zátěží plynoucí z žádostí o dotaci je velmi náročné přesvědčit soukromého podnikatele o investici.

V souvislosti s I. výzvou NKÚ v roce 2020 poukázalo na fakt, že MPO nevyplatilo žádné dotace na budování sítí pro vysokorychlostní internet. MPO selhalo v nastavení podpory a nedostatečné přípravě programu [10].

Druhá výzva Vysokorychlostní internet byla vypsána v roce 2019. IV. Výzva Vysokorychlostní internet byla vypsána v roce 2020, v rámci této výzvy nebyly příjemci obce. V rámci výzvy II. a IV. získal podporu pro kraj Vysočina subjekt CETIN, a.s. IV. MPO zveřejnilo, že v rámci OP PIK bylo podpořeno cekem 135 obcí. Pokud se podíváme na konkrétní data, tak největší podpora mířila do Plzeňského a Středočeského kraje. Ve výzvě nebyla podpořena žádná obec z krajů Olomouckého, Libereckého, Pardubického a Karlovarského. Nízký počet obcí byl podpořen v Ústeckém a Moravskoslezském kraji [11].

Další výzvy, které je cílené na podporu rozvoje konektivity v obcích jsou vypisovány v rámci Národního plánu obnovy. V současní době je vypsána III. Výzva Digitální vysokokapacitní sítě z Národního plánu obnovy pro podporu budování infrastruktury základnových stanic sítí 5G. Finanční podpora je zaměřena na výstavbu technické infrastruktury v investičně náročných lokalitách, tedy venkovských oblastech.

Analýza konektivita – TOP země EU

Za předpokladu, že se na řešení konektivity díváme z pohledu globální ekonomiky, tak je možné uvést si příklady a specifika zemí, které jsou z hlediska konektivity v rámci EU nejúspěšnější. Nutno podotknout, že každá země disponuje odlišnými socio-ekonomickými faktory a lze předpokládat, že není vždy možné implementovat zcela totožné řešení pro dosažení stejného úspěchu.

Podle DESI indikátoru se v oblasti konektivity nacházelo v roce 2021 před Českou republikou celkem 16 států [6]. Nejlepšími pěti státy podle stejného indexu bylo Dánsko, Nizozemsko, Španělsko, Německo a Itálie. Sousední země ČR skončily na 25. místě (Polsko), 21. místě (Slovensko) a na 15. místě (Rakousko) [4].

V rámci DESI indexu vykazuje nejlepší výsledky v oblasti konektivity Dánsko. Země dosahuje nadprůměrných výsledků v kategoriích: 95 % domácností je pokryto VHCN, 74 % domácností je pokryto optickou sítí FTTP, přičemž Dánsko exceluje v pokrytí venkovských oblastí a 98 % osídlených oblastí je pokryto sítí 5G. Dánsko schválilo na konci roku 2021 strategii, ve které si stanovilo cíl pokrytí všech domácností a podniků rychlostí 100/30Mbs a zároveň 98 % z nich musí být pokryto sítí s rychlostí 1Gbps. Oba cíle jsou stanoveny do roku 2025 [12].

Druhou zemí v oblasti konektivity je Nizozemsko. 91 % země je již pokryto pevnými sítěmi s velmi vysokou kapacitou (VHCN) a pokrytí 5G v obydlených oblastech dosahuje 97 %.

Další zemí na špici konektivity je Španělsko. To dosahuje obzvláště dobrých výsledků v oblasti pokrytí pevnou sítí s velmi vysokou kapacitou (VHCN) (94 % oproti průměru EU 70 %), zatímco v oblasti pokrytí 5G je pouze průměrné, a to zejména kvůli určitému zpoždění při dražbě všech průkopnických pásem 5G.

Státem, který leží u hranic České republiky a jež má podle indexu DESI nejvyšší míru konektivity je Německo. To je zároveň čtvrté v pořadí v celé EU ve stejné oblasti. Německo dosáhlo 96% pokrytí rychlým širokopásmovým připojením, což poskytuje dobrý základ pro digitální zapojení do společnosti a ekonomiky. Nicméně, i přes to, že se pokrytí venkova od roku 2019 výrazně zlepšilo, a to z 75 % na 85 %, což je výrazně nad průměrem EU, který činí 67,5 %, tak Německo stále vykazuje zřetelnou digitální propast mezi městskými a venkovskými oblastmi [13].

Proč mají některé státy lepší konektivitu?

Jedním z přístupů, jak výrazně zlepšit konektivitu v rámci regulatorních nařízení je povinnost poskytovatelů a provozovatelů internetového připojení zajistit určité procentuální pokrytí země. Jedním z takových případů je Nizozemsko, kde je licence na pásmo 700 MHz v rámci 5G sítě spojeno s povinností 98 % pokrytí mobilními sítěmi [14]. Podobný přístup má také Španělsko, které zavazuje operátory (Telefónica, Orange a Vodafone) využíváním pásma 700 MHz povinnost pokrýt vysokorychlostním internetem přístavy, nádraží, silnice, a tím přispět k rychlému rozšíření 5G sítě [15].

Klíčovou částí při rozšiřování konektivity jsou investice, a to jak soukromé, tak z veřejných rozpočtů. Pro městské oblasti jsou z velké části pokryty internetem z investic ze soukromých zdrojů. Situace je ovšem odlišná zejména ve venkovských oblastech, kde je menší hustota osídlení. Většina států se silnou konektivitou má fondy a programy na podporu rozšíření (vysokorychlostního) internetového připojení.

První příčka Dánska v oblasti konektivity je dosažena i díky poměrně hustému pokrytí vysokorychlostním internetem ve venkovských oblastech. Jedním efektivních kanálů, přes který Dánsko výrazně modernizuje svoji internetovou síť, je instituce Národní širokopásmý fondu (National Broadband pool), který se zaměřuje na financování pro zavádění vysokokapacitního širokopásmového připojení v méně dostupných oblastech. V roce 2022 tomuto fondu byly přiděleny prostředky ve výši 13,5 mil. Eur [16].

Podobně jako v ostatních státech EU se snaží investice do konektivity zlepšit socioekonomické prostředí i méně rozvinutých oblastí. Jedním z takových programů v Německu tzv. Digitální třída [17], která je samostatný program a má za cíl podpořit připojení škol k širokopásmovým sítím. Celkem je financováno přibližně 11 700 škol. Dalším finančním programem německé spolkové vlády je financování mobilních sítí, na který je uvolněn rozpočet před 1 miliardu eur. Cílem těchto subvencí je zajistit mobilní sítě 5G v odlehlých nebo alespoň 4G v tzv. bílých místech, tedy oblastech, která mají pouze 2G možnost připojení nebo nemají žádné [13].

Vysokého stupně pokrytí VHCN bylo ve Španělsku dosud dosaženo především díky soukromým investicím. Veřejné finanční prostředky, především prostředky RRF, jsou nyní vyčleněny na zavádění sítí 5G a VHC, zejména ve venkovských oblastech [15]. Španělsko se rozhodlo podporovat nejen investice do infrastruktury, ale také poptávku po vysokorychlostním internetovém připojení. Jedním z kroků, které Španělsko podniklo, byla podpora v zavedení širokopásmového připojení v rámci španělského RRP projektu v hodnotě 30 milionů EUR. Součástí tohoto projektu byly také poukázky na připojení, které byly dočasně poskytovány znevýhodněným skupinám obyvatelstva [18].

Nutno podotknout, že jsou i výjimky – například v Nizozemsku neexistuje historicky žádný národní financování širokopásmového připojení a hlavní hybnou silou v zavádění internetových sítí byly soukromé investice [14]. To může být také důvodem, že Nizozemsko výrazně zaostává s pouhými 33 % přiděleného pásma 5G ve srovnán s 56 % – průměrem EU.

Lze pozorovat v zemích, které jsou na předních místech v oblasti konektivity, že vyšší míra konkurenčního prostředí koreluje s rozšířeností internetu v dané zemi. Silnější konkurenční prostředí tak například ve Španělsku umožnilo v předchozích letech výrazné rozšíření širokopásmového připojení, zejména během pandemie COVID-19, a to díky zvýšené poptávce po širokopásmových produktech (většinou v balíčcích) a placených televizních službách [15].

Diskuze

Pro řešení problematiky mobilních sítí by mohla být vhodná inspirace úspěšných zemí. Zásadními aspekty, kterými státy vykazující nejlepší výsledky v oblasti konektivity disponují, jsou efektivní investice do infrastruktury a podpoření nabídky. Dále je důležité, aby bylo zajištěno adekvátní konkurenční prostředí, které vede k vyšším soukromým investicím do infrastruktury i služeb. Toto má za následek snížení cen pro koncové zákazníky. Tyto státy přidělují pásma pro 5G sítě, čímž vytváří povinnost soukromých operátorů zajistit velmi vysoké pokrytí státu internetovým připojením.

Řešení otázek, které se týkají vysokorychlostního internetového připojení bílých míst je velmi specifické a vyžaduje hlubší zamyšlení. Tam, kde, již bylo pro soukromý sektor výhodné investovat, tak taková místa jsou již pokryta. V případě bílých míst se jedná o lokality, u nichž implementaci doprovází bariéry a pro soukromý sektor není příliš výhodné budovat potřebnou technickou infrastrukturu k zavedení sítě. V takovém případě zůstává na státu, aby těmto lokalitám k potřebné implementaci pomohl. I přes poměrně vysoký počet výzev, který byl ze strany MPO iniciovaný, se stále nedaří na tyto lokality zacílit. Co může být příčinou, že se v rámci výzev MPO stále nedaří oslovit cílené žadatele? Respektive proč se obec, jakožto veřejnoprávní korporace, do výzev vysokorychlostního internetu příliš nezapojuje?

Jak již upozornilo NKÚ, některé výzvy jsou příliš náročné a špatně uchopitelné. Oslovujeme obce s nízkým počtem obyvatel, které jsou specifické nízkými příjmy a nízkým personálním zajištěním. Domnívám se, že ve spojení s administrativní náročností výzev je pro některé starosty neefektivní o danou dotaci žádat. Pokud se podíváme na příjmy menších obcí, tak v případě neúspěšné žádosti o dotaci vyplácené ex-post, by tato částka obec zadlužila na dlouhé období. Obce k přípravě žádostí často využívají služeb poradenských firem. Nicméně i tak Vám poradenská společnost nemůže zaručit, že ve výzvě skutečně uspějete. Nikdo nechce být ten, kdo obec zatíží dluhovým břemenem s nejistotu adekvátní efektivnosti a návratnosti. Myslím si, že dalším problémem může být nedůvěra starostů v systém čerpání dotací díky předchozí neúspěšně podané žádosti.

Další otázkou je samotná neinformovanost o aktuálních dotacích. Vzhledem k tomu, že cílíme na obce, kde je nedostatečné internetové připojení a většinou tedy i úřad jím nedisponuje, tak je obtížné se o samotné dotaci dozvědět. V mnoha oblastech si tuto roli informátora přebírá MAS. Ta dokáže zástupcům obcí efektivně předložit stávající dotace, na které je možné čerpat a zároveň jim je předá pochopitelnějším způsobem. Otázkou zůstává, zda by nebylo efektivnější vytvořit edukativní kurzy pro zástupce a zaměstnance MAS, kteří mají k místním lokalitám skutečný vztah a znají jejich skutečné problémy a potřeby. V rámci

doktorského studia jsem se zapojila do mezinárodního projektu, který na tyto problémy při čerpání dotací taktéž poukazoval. Zároveň bylo znatelné, jak vysokou důležitost MAS pro některé obce v rámci informovanosti o dotačních titulech hrají.

Pokud skutečně chceme zefektivnit čerpání dotací pro obce, u kterých je to nejvíce potřeba, tak je nutné vzít v potaz personální zajištění. Myslím si, že starostové těchto obcí nemusí mít bližší zkušenosti s čerpáním dotací a vzhledem k administrativní náročnosti se následně o dotace nemusejí pokoušet. K zefektivnění může pomoci tvorba on-line aplikace, ve které obce naleznou příklady k vyplnění, rady a tipy a případně možnost chatbota. Tuto aplikaci by následně mohly využívat i MAS, které s dotacemi obcím a drobným podnikatelům pomáhají.

Závěr

Internetové připojení hraje významnou roli pro digitální transformaci ekonomik. Evropská unie každoročně analyzuje oblast digitálního rozvoje jednotlivých členských států pomocí indexu DESI. Česká republika v oblasti konektivity v indexu DESI 2022 obsadila 17. místo. Zároveň ve všech čtyřech oblastech, které DESI zkoumá, je oblast konektivity v ČR hodnocena nejhůře. Zásadními problémy je nízké využití vysokorychlostního připojení, nízké pokrytí optickou sítí FTTP a sítěmi s velmi vysokou kapacitou a drahé ceny za mobilní sítě. Na řešení výstavby technické infrastruktury se podílí soukromý sektor a poté stát. Česká republika na základě dokumentů EU přijala řadu opatření a iniciativ pro rozvoj vysokorychlostního internetového připojení.

Práce se blíže zaměřila na specifické problémy ČR v podobě vysokých cen a 5G sítě a poté kontroverzi vypisovaných výzev MPO na řešení pokrytí bílých míst. I přes nižší pokrytí 5G sítí v ČR jsme významně nad průměrem pokrytí ve venkovských oblastech. Specifické problémy související s 5G sítěmi byly vymezeny jako: nedostatečná konkurence v oblasti telekomunikací a nedostatečné pokrytí území. MPO iniciuje výzvy na podporu konektivity v obcích pomocí OP Podnikání a inovace, skrz který byly v programovacím období 2014-2020 vypsány 4 výzvy. Bohužel i přes značný objem peněz, který byl na pokrytí vysokorychlostním internetem vyčleněn se nepodařilo bílá místa ve vysoké míře pokrýt. Specifickou otázkou k dalšímu zkoumání zůstává, proč některé příhraniční kraje, kde nalezneme vysokou koncentraci bílých míst nebyly ve větší míře podpořeny.

Pro identifikování příkladů dobré praxe byla analyzována konektivita u zemí, které vykazují nejlepší výsledky v rámci indexu DESI. U těchto států nalezneme některé shodné aspekty, které výrazně pomáhají zlepšovat jejich celkové pokrytí internetovým připojením. Zásadními aspekty jsou efektivní investice do infrastruktury i podpoření nabídky, zajištění konkurenčního prostředí, které vede k vyšším soukromým investicím do infrastruktury i služeb a má za následek také snížení cen pro koncové zákazníky. Dále tyto státy přidělují pásma pro 5G sítě, čímž vytváří povinnost soukromých operátorů zajistit velmi vysoké pokrytí státu internetovým připojením.

Řešení otázek konektivity v bílých místech je velmi specifické a k uchopení problému je třeba, abychom provedli hlubší analýzu a problematiku pochopili přímo od starostů těchto oblastí. Domnívám se, že problémem může být příliš vysoká administrativní náročnost a špatná uchopitelnost výzev. Obce disponuji nižšími financemi a v případě neúspěšného žádání o dotace by se zadlužili na dlouhé období. Otázkou zůstává, zda probíhá dostatečná informovanost o vypsání dotace a zda MPO dokáže žadatele správně oslovit. Zejména pokud se v dnešní době jedná o jeden ze základních komplementů, jako je internetové připojení. Zásadní roli v informovanosti dokáží ve specifických lokalitách předat funkční MAS. Domnívám se, že edukace či vytvoření on-line nástrojů pro ulehčení podávání žádostí by dokázala v úspěšnosti oslovení specifických skupin pomoci. Nicméně, tato otázka vyžaduje hlubší analýzu a do budoucna je potřebné hledat řešení se zástupci těchto míst.

Literatura

[1] Solomon, J., & Klyton, M. (2020). The Impact of Mobile Phones on Social Interaction. International Journal of Humanities and Social Science Research, 8(2), 26-33, Evangelista, F., Laperchia, A., Pellegrini, M. M., & Coluccia, A. (2014). An integrated approach to mobile advertising: the effect of mobile, social and location-based techniques on advertising response metrics. Journal of Business Research, 67(11), 2525-2532.

[2] Hernandez, J. M. C., Munoz-Gallego, P. A., & Aguado, J. M. G. (2016). The Impact of Social Media on Consumer Behavior: An Empirical Study on Factors Influencing Consumer Purchase Intention in China Under the Social Media Context. Journal of Business Research, 69(8), 3047-3052

[3] Kenney, M. (1995). The transfer of Japanese manufacturing techniques to the US: context, process and outcomes. Journal of Management Studies, 32(2), 151-171.

[4] Evropská komise. Index digitálního hospodářství a společnosti (DESI) [online]. [citováno 22. 4. 2023]. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/desi.

[5] Český statistický úřad. (2022). Investice v ICT. [online]. [citováno 23. 4. 2023]. Dostupné z: https://www.czso.cz/csu/czso/investice_v_ict.

[6] Evropská komise. (2022). Digital Economy and Society Index (DESI) 2022 country report - Czechia. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88743.

[7] Česká telekomunikační agentura. (2021). Zpráva o vývoji a situaci v oblasti elektronických komunikací za rok 2020. [online]. [citováno 30. 4. 2023]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/stranky/8179/soubory/zovt-2021.pdf.

[8] Evropská komise. (2022). Mobile and Fixed Broadband Prices in Europe 2021. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88311.

[9] ČTÚ. (2022). ZPRÁVA O VÝVOJI TRHU ELEKTRONICKÝCH KOMUNIKACÍ SE ZAMĚŘENÍM NA ROK 2021. [online]. [citováno 20. 4. 2023]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/stranky/8179/soubory/zovt-2021.pdf.

[10] NKÚ. (2022). Na vysokorychlostní internet nevyplatil stát za pět let žádné dotace. Pokrytí rostlo jen díky investicím podnikatelů. [online]. [citováno 20. 4. 2023]. Dostupné z: https://www.nku.cz/cz/pro-media/tiskove-zpravy/na-vysokorychlostni-internet-nevyplatil-stat-za-pet-let-zadne-dotace--pokryti-rostlo-jen-diky-investicim-podnikatelu-id11266/.

[11] MPO. (2022). Seznam obcí, které získaly dotace na vysokorychlostní internet. [online]. [citováno 20. 4. 2023]. Dostupné z: https://www.mpo.cz/cz/rozcestnik/ministerstvo/aplikace-zakona-c-106-1999-sb/informace-zverejnovane-podle-paragrafu-5-odstavec-3-zakona/seznam-obci--ktere-ziskaly-dotace-na-vysokorychlostni-internet--273691/.

[12] Evropská komise. (2022). Digital Economy and Society Index (DESI) 2022 country report - Denmark. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88699.

[13] Evropská komise. (2022). Digital Economy and Society Index (DESI) 2022 country report - Germany. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88702

[14] Evropská komise. (2022). Digital Economy and Society Index (DESI) 2022 country report - Netherlands. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88695.

[15] Evropská komise. (2022). Digital Economy and Society Index (DESI) 2022 country report - Spain. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88720.

[16] Evropská komise. (2022). Digital Economy and Society Index (DESI) 2022 country report - Denmark. [online]. [citováno 20. 4. 2023]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/88699.

[17] DIGITALPakt Schule. Breitbandanschluss für Schulen [online]. DIGITALPakt Schule, [cit. 2023-04-30]. Dostupné z: https://www.digitalpaktschule.de/de/breitbandanschluss-fur-schulen-1742.html.

[18] BOLETÍN OFICIAL DEL ESTADO. Real Decreto-ley 8/2021, de 4 de mayo, por el que se adoptan medidas urgentes en el ámbito de la vivienda y la renta de alquiler [online]. 5 May 2021 [cit. 2023-04-30]. Dostupné z: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-18817

Zase závěrečný účet. A zkusili jste MIS?

Ing. Andrea Hlávková, Produkt Manager VERA, spol. s r.o.

Uzávěrky ve městech jsou konečně zpracovány a odeslány. Nastává další náročná fáze nejenom pro vedoucí finančních odborů, ale pro celé vedení města. Musí se připravit Závěrečný účet – a to je spousta práce. Potřebujete detailní výstupy dle odborů, příspěvkových organizací, množství přehledů o přijatých a poskytnutých dotacích, o stavech finančních prostředků atd. Tyto obsáhlé informace se sice nacházejí standardně v informačním systému, ale jsou roztroušené v různých agendách. Jejich sesbírání a zpracování do vhodných výstupů zabírá dny až týdny času. Pojďte to dělat jednodušeji.

Většinu potřebných podkladů naleznete v Manažerském informačním systému VERA Radnice (MIS) a to nejenom formou tabulek, ale i v grafech, které lze stáhnout a bez dalšího zpracování přímo použít jak pro Závěrečný účet, tak pro další účely. Všechny důležité informace máte k dispozici v reálném čase.

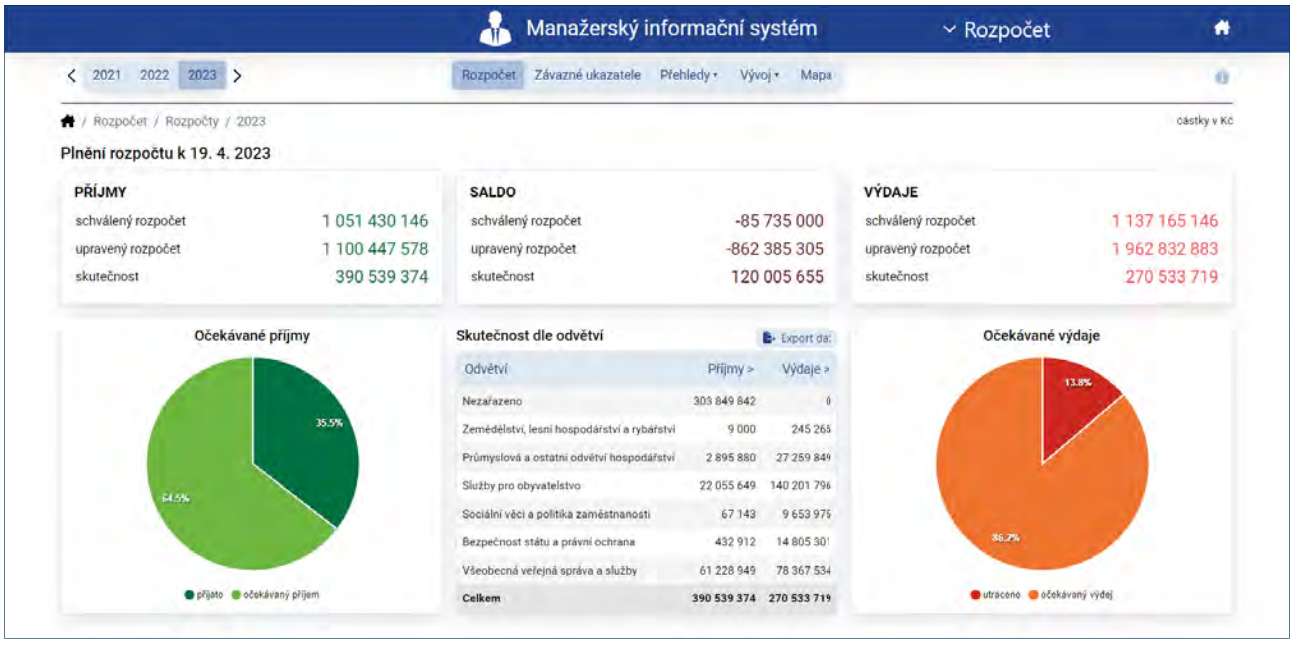
Pro koho se MIS hodí?

MIS je webovou aplikací a přístup do něj lze nastavit nejen pro vedení obce a vedoucí zaměstnance, ale např. i pro členy finančního výboru nebo zastupitele, aby měli přehled o fungování obce. Všechny informace, které MIS zobrazuje jsou v souladu se zákonem na ochranu osobních údajů a GDPR.

MIS má jednoduché použití, je intuitivní a nabízí komplexní data pocházející z různých zdrojů na jednom místě a tím úsporu času spojenou s vyhledáváním potřebných údajů v různých agendách.

Jaké konkrétní informace MIS nabízí?

- čerpání a plnění rozpočtu dle vybraných kritérií např. dle odborů, závazných ukazatelů, rozpočtových položek, oddílu a paragrafu nebo projektů,
- přehled pohledávek – jejich aktuální stav, měsíční vývoj jednotlivých druhů pohledávek, meziroční vývoj za posledních 5 let, včetně informací o stavu vymáhání pohledávek, tj. kolik je zahájeno řízení, stavy jednotlivých úkonů vymáhacího řízení, kolik řízení bylo ukončeno ...
- přehled závazků – jejich aktuální stav, měsíční vývoj jednotlivých druhů výdajů, meziroční vývoj za posledních 5 let, přehledy všech přijatých faktur a vystavených výdajových poukazů dle partnerů (dodavatelů) s rozpadem až na jednotlivé doklady,
- přehled poskytnutých dotací dle jednotlivých oblastí (sportovní, kulturní, sociální, ...) včetně informací o počtu přijatých žádostí, o požadované výši dotací i výši alokovaných prostředků, přehled jednotlivých žadatelů a jejich meziroční srovnání za posledních 5 let,
- přehledy o finančních prostředních – stavy a vývoj jednotlivých fondů, bankovních a úvěrových účtů.

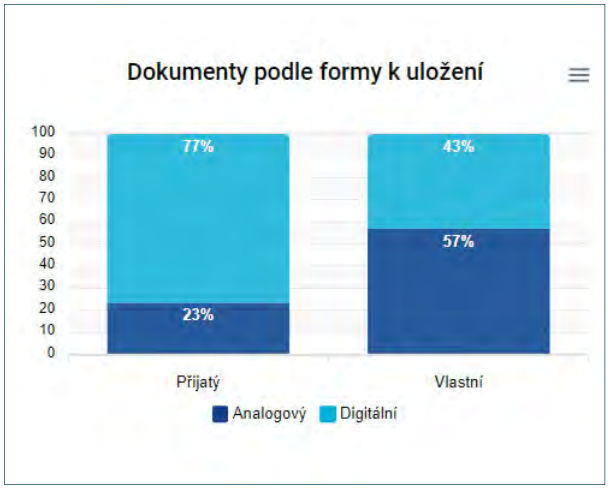


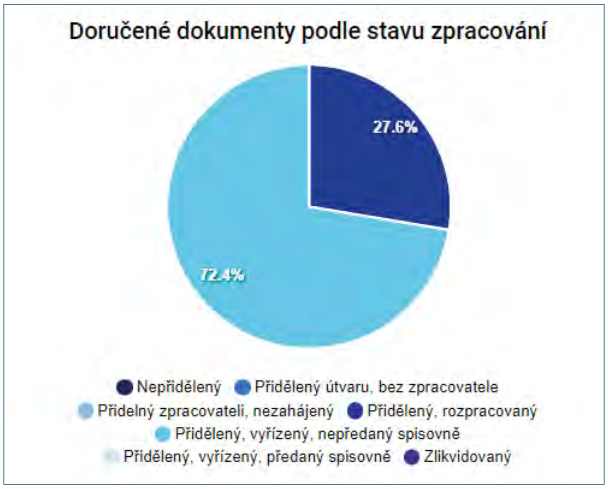
Pro jaké další účely (mimo přípravy Závěrečného účtu) lze MIS využít?

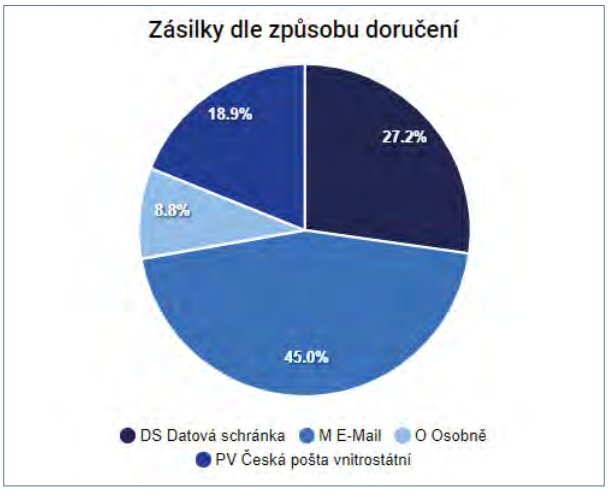
- pokud chce být obec vnímána jako transparentní vůči veřejnosti, může z MISu exportovat různé výstupy a prezentovat je na webu obce, v místních tiskovinách, sociálních sítích a v ostatních médiích,
- nabízené tabulkové i grafické výstupy lze vyexportovat a vložit do podkladových materiálů a průběžných zpráv o hospodaření obce pro jednání rady, zastupitelstva nebo jiných orgánů obce,
- při auditu jsou k dispozici požadované informace bez zdlouhavých příprav a dohledávání,
- při zpracování statistických výkazů pro ČSÚ a pro tvorbu vlastních statistických přehledů,
- při zpracování analýz a podkladů pro strategické rozhodování,
- při vyhodnocování realizovaných akcí a projektů.

Týká se MIS pouze ekonomiky?

Kromě informací o hospodaření obce nabízí MIS i údaje o spisové službě. Uživatel-manažer má přehled o tom, kolik dokumentů bylo na úřad přijato a v jaké formě, a naopak kolik a v jaké formě bylo z úřadu vypraveno. Zjistí tak vytíženost jednotlivých odborů i to, kolik písemností bylo vyřízeno, kolik spisů bylo uzavřeno a kolik jich bylo předáno do spisovny a jak je na obci využívána možnost digitálního vypravení dokumentů. Zároveň má přehled, kolik má úřad vyčerpaných časových razítek.







Chcete vidět, jak to funguje? Požádejte obchodní zástupce VERA o prezentaci. Rádi Vám ukážeme výstupy v praxi.

www.vera.cz, info@vera.cz

*Společnost **VERA** se od roku 1994 věnuje vývoji a implementaci informačních systémů pro veřejnou správu. Jednotný systém klientům zastřeší oblast ekonomiky, spisové služby, správních agend, manažerských nadstaveb, komunikaci s občanem (Portál občana), interní procesy úřadu, zpracování přestupků z kamerových systémů, řešení pro městskou policii a další.*

VERA poskytuje celou řadu služeb, které souvisí s využíváním softwaru a garantuje svým klientům vývoj v souladu s platnou legislativou. Je držitelem certifikátů ISO 9001:2015, ISO 27001:2013 a aktivním členem ICT UNIE.

Pohled původce na připravované atestace spisových služeb

Pavel Jirásek, MČ Praha 16
Tomáš Lechner, TRIADA, spol. s r. o.

Role spisové služby v úřadu

Elektronické systémy spisové služby jsou nedílnou součástí rozvoje elektronizace veřejné správy. Jejich legislativní zavedení bylo spojeno s nástupem komunikace prostřednictvím datových schránek s cílem zajistit důvěryhodnou správu přijatých elektronických dokumentů a efektivní tvorbu vlastních dokumentů rovnou v elektronické podobě včetně jejich případného následného odeslání přes datovou schránku. Historicky navazují elektronické systémy spisové služby na obecné principy založené na přírůstkové evidenci podacího deníku v listinné podobě. Nicméně elektronizace mění pohled na to, co spisová služba vlastně je. Nyní již nedokladuje jen příjem a odeslání dokumentů, ale stará se o celý životní cyklus dokumentů včetně jejich uložení ve spisovně po dobu běhu skartační lhůty. Elektronické systémy spisové služby nejsou tedy jenom dokumentačním doplňkem, ale základním nástrojem pro úřadování, byť někdy vystupujícím v roli podpůrného nástroje na pozadí úředních procesů.

Možná i tento posun v úloze spisové služby vedl k tomu, že v roce 2021 byla uzákoněna atestace elektronických systémů spisových služeb. Primárním cílem bylo zřejmě zkvalitnění výkonu spisové služby, ale nelze se v tomto ohledu opřít o důvodovou zprávu k zákonu, protože atestace byla do zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, přidána až pozměňovacím poslaneckým návrhem. Nicméně je otázkou, zda atestace jako takové automaticky zajistí kvalitnější a spolehlivější chod spisové služby v elektronické podobě, nebo půjde jen o další zbytečnou administrativní a finanční zátěž. Navíc nastavená pravidla pro atestace mohou vést k významné nejistotě plynoucí z poměrně krátké doby platnosti atestu ve srovnání s tím, jak dlouho může trvat kvalitní nasazení spisové služby v organizaci.

Ač by se mohlo zdát ve srovnání se soukromým sektorem, že veřejná správa je dlouhodobě stabilní, tak množství legislativních změn regulujících výkon veřejné správy a také její postupující elektronizace v reakci na dynamický rozvoj informační společnosti působí, že je třeba se vyrovnávat s řadou dílčích změn, které se musí promítnout také do spisové služby. Dalším významným prvkem, který je třeba pro správnou implementaci elektronické spisové služby zohlednit, je množství specifických agendových informačních systémů či informačních systémů spravujících dokumenty, které by měly být v ideálním případě provázány na centrální spisovou službu úřadu. Proto nasazení spisové služby a její rozvoj v organizaci je dlouhodobý, vlastně až nikdy nekončící, příběh. Z tohoto pohledu je délka platnosti atestu a pravidlo, že systém, který neprošel reatestací, musí původce nahradit do jednoho roku atestovaným systémem v praxi pro mnoho organizací, zejména těch větších, naprosto nerealizovatelný.

Atestace spisových služeb

Původně nastavený plán zavedení atestace elektronických systémů spisové služby byl v loňském roce upraven. Podle aktuálně platného itineráře se elektronické systémy spisové služby začnou atestovat 1. července letošního roku. Vybraným atestačním střediskem je Česká agentura pro standardizaci, která by do té doby měla zveřejnit atestační scénáře, které budou součástí provozního řádu atestačního střediska, jak na konci ledna tohoto roku stanovilo Ministerstvo vnitra.

Od 1. července 2024 má platit zákaz nabízet nebo dodávat neatestované elektronické systémy spisové služby. To je tedy okamžik, do kterého by každý původce měl prověřit, že právě jeho dodavatel spisové služby získal pro svůj systém atest. A pokud náhodnou ne, musí se rychle dívat jinde, protože už má jen 1,5 roku, než bude platit povinnost využívat jen a pouze atestované systémy spisové služby.

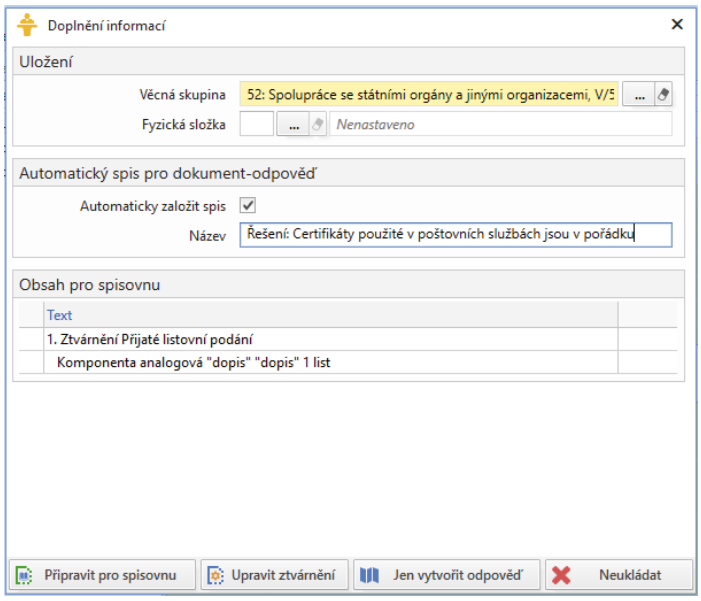
Zopakujme ještě jednou fakt, že atest konkrétního elektronického systému spisové služby bude platit nejvýše dva roky, pokud nedojde ke změně předpisů, podle nichž byl atest proveden. V takovém případě se délka atestu zkracuje tak, že jeho platnosti skončí nejpozději do roka od nabytí účinnosti případných změn těchto předpisů. Znamená to, že elektronické systémy spisové služby, které získají atesty v určené době do 1. července 2024, budou muset být velmi brzo po začátku platnosti povinnosti jejich použití původci (1. ledna 2026) opět reatestovány. Z pohledu nastavených termínů to budou všechny elektronické systémy spisové služby, jejichž dodavatelé chtějí zůstat působit na tomto trhu a spisové služby dále dodávat. Tato skutečnost rozhodně nepřidá na klidu nikomu, kdo je za vedení spisové služby v organizacích veřejné správy zodpovědný, protože jistota kvalitního nástroje podložená atestem z roku 2024 bude muset být opakovaně prověřena právě v okamžiku nástupu povinnosti takové systémy používat.

Elektronická spisová služba Munis ERMS

Společnost Triada, která je tvůrcem i dodavatelem elektronického systému spisové služby Munis ERMS, se samozřejmě aktivně připravuje na budoucí atestace svého systému a sleduje dění kolem připravovaných změn předpisů. Dne 13. dubna letošního roku vyšla ve sbírce zákonů novelizace vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, což znamená, že je známa finální podoba první poloviny z celkové dávky změn, která se v rámci přípravy na atestace očekává. Druhou polovinou bude národní standard pro elektronické systémy spisové služby, který má být také významně změněn.

Mezi nejvýraznější již zveřejněné změny patří zvýšení role jednoznačného identifikátoru dokumentu, který postupně v některých procesech nahrazuje stávající základní evidenční označení dokumentů v podobě čísla jednacího, povinné vkládání dokumentů do spisu nejpozději v okamžiku, kdy se začnou vyřizovat, což ruku v ruce znamená změnu pohledu na spisy, která se více přibližuje správnímu řádu. Nicméně bohužel nebyl při příležitosti práce na změnách ve spisové službě řešen dlouhodobý rozpor pohledu na spisy v různých procesních právních předpisech, např. mezi správním a daňovým řádem, takže zůstal při starém i dvojí pohled na číslování spisů, byť už se mu přímo neříká priorace a sběrný arch.

Povinným vkládáním dokumentů do spisů se sjednocují postupy při vyřizování dokumentů, byť to znamená zákaz jednoduchého vzetí na vědomí či odpovědi bez tvorby spisu. V této souvislosti lze poukázat na to, jak se elektronická spisová služba Munis ERMS připravuje na tyto změny, protože záměr zavést tuto povinnost byl avizován již mnohem dříve. Elektronická spisová služba Munis ERMS má již více než dva roky aplikovánu automatickou tvorbu spisů pro dvojice dokumentů podání – odpověď, čímž i uživatele vychováváme k tomu, aby zmíněná změna povinné tvorby spisů nebyla zas tak velká.



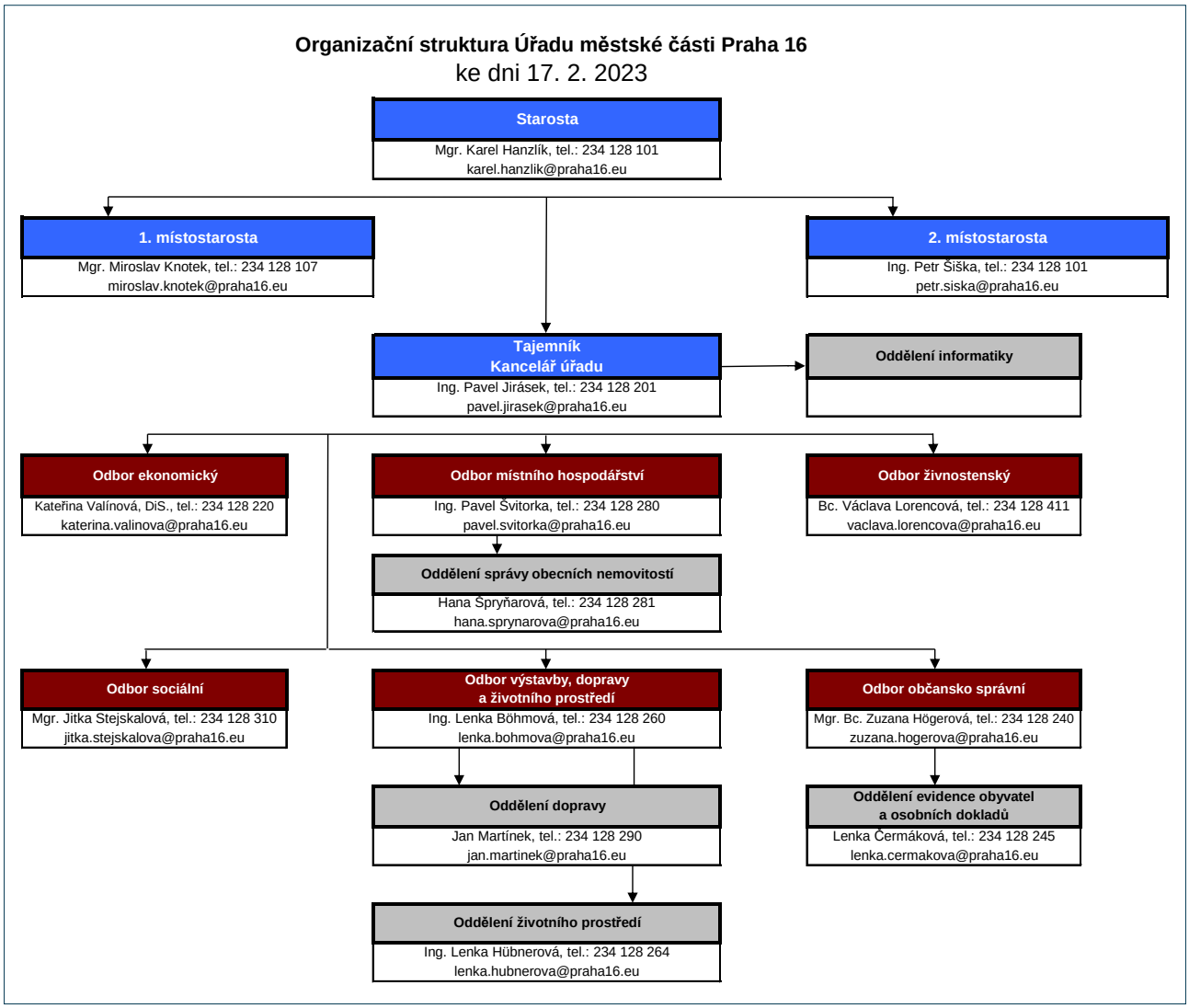
Obr. 1: Ukázka automatické tvorby spisu při odpovědi na podání.

ÚMČ Praha 16

Hlavní město Praha je členěno na 22 správních obvodů a 57 městských částí. Městská část Praha 16 (ilustrativní fotografie viz Obr 2) je jednou z těchto částí ležící na jihozápadním okraji města. Současně je sídlem správního obvodu, který zahrnuje území městských částí Praha 16 (katastrální území Radotín), Praha - Lipence, Praha - Lochkov, Praha - Velká Chuchle (katastrální území Velká Chuchle a Malá Chuchle) a Praha - Zbraslav (katastrální území Zbraslav a Lahovice). Celý správní obvod měl k 1. lednu 2023 celkem 23 064 obyvatel (z toho v Radotíně 7 801) při rozloze 3 616 ha (z toho Radotín 931 ha). Další informace o městské části lze najít na webových stránkách [1].

Úřad městské části Praha 16 je členěn na odbory, jejichž úkolem je vykonávat státní správu (u většiny agend pro celý správní obvod) a samosprávu (pouze pro Radotín) dle Organizačního řádu úřadu, případně dle pověření Rady městské části tak, aby byla zajištěna činnost úřadu jako orgánu městské části. Aktuální podobu organizační struktury představuje schéma na Obr. 3.

Obr. 2: Letecký snímek Prahy 16 – autor Ing. Pavel Jirásek.



Obr. 3: Organizační schéma ÚMČ Praha 16, zdroj [1].

Diskuse

Úřad MČ Praha 16 vede elektronickou spisovou službu od začátku zavedení tohoto legislativního pojmu a v návaznosti na již dřívější využívání možností informačního systému Munis pro podporu výkonu spisové služby. Elektronická spisová služba Munis ERMS je využívána všemi 80 uživateli úřadu, byť v některých případech nepřímo prostřednictvím vazby z propojených agend výstavby, dopravy a životního prostředí. Spisová služba pro nás znamená klíčový prvek administrativních procesů, nezbytnou oporu mající dosah do všech agend a činnostních rolí v rámci zákony či Statutem hlavního města Prahy svěřených kompetencí v samostatné i přenesené působnosti. Bez spolehlivé a kvalitní elektronické spisové služby si dnes již nikdo nedokáže představit chod jakéhokoli orgánu veřejné moci v České republice.

Pro bezproblémový výkon spisové služby jsme v úzkém kontaktu s dodavatelem, u něhož objednáváme pravidelná školení rozšiřující znalosti uživatelů a navazující na aktualizace užívaného informačního systému. Takovým prubířským kamenem v oblasti implementace elektronické spisové služby je provedení elektronického skartačního řízení. V současné době máme již za sebou

tři takováto řízení a připravujeme se na čtvrté. V posledním dokončeném řízení bylo navrženo a tímto řízením prošlo celkem 4139 samostatných dokumentů a 373 spisů.

Atestace elektronických systémů spisových služeb je z pohledu původce teoreticky možností mít určitou jistotu o kvalitě dodavatele a jeho spolehlivosti, na stranu druhou způsob jejího schválení i první informace o průběhu samotného atestačního procesu spíše naznačuje, že se bude jednat o další administrativní, časovou a finanční zátěž, kterou dodavatelé informačních systémů zákonitě v konečném důsledku přenesou na odběratele. Věřme, že toto je jen nejhorší možný scénář a že v reálném procesu atestace přeci jen pomohou a zkvalitní elektronické služby ve veřejné správě.

Literatura

[1] Oficiální webové stránky městské části Praha 16, dostupné na <https://www.praha16.eu/>.

Spisová služba – živá součást agend a oběhu dokumentů

Ing. Michal Kellner, Allium, s.r.o.

Spisová služba bývá někdy spíše strašákem a nepříliš oblíbeným nástrojem. Nemusí tomu tak ale být. Naučme se ji využívat, propojme ji s jinými systémy a využijme její funkce i pro dokumenty, které dnes primárně tvoříme a ukládáme v jiných systémech nebo agendách.

K čemu je nám vlastně spisová služba? A používáme ji skutečně správně?

Malé připomenutí na úvod – spisová služba se stará nejen o správné třídění, evidenci a archivaci dokumentů. Moderní systémy spisové služby dnes nabízí i další zajímavé funkce, které lze u agendových dokumentů s výhodou využít. Ať už je to kontrola elektronických podpisů, příjem nebo odesílání datových zpráv a další.

Agendy? Agendové dokumenty? Co to je? V organizacích vzniká velké množství elektronických informací, a to navíc v různých systémech. To ale neznamená, že tyto informace nemají být ve spisové službě evidovány nebo že s nimi nemá být správně pracováno. Jak nakládat s dokumenty a které dokumenty mají být součástí spisové služby popisuje zákon č. 499/2004 Sb. o archivnictví a spisové službě a vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby. Nesmíme tak zapomínat, že touto právní úpravou se řídí také například správa těchto typů dokumentů:

- Smlouvy a dohody, právní dokumentace a analýzy
- Faktury a účetní dokumentace
- Personální dokumentace
- Další interní a externí komunikace, předpisy a řízená dokumentace

Může nám spisová služba skutečně pomáhat? Jak?

Může, a to nejen v oblasti uspořádání dokumentů a podpory jejich životního cyklu včetně tvorby, schvalování, seznámení s obsahem, archivací.

S rozvojem digitalizace a elektronické komunikace stále častěji využíváme elektronické podepisování. A právě podpora elektronických podpisů a jejich validace je jednou z velmi užitečných funkcí. Určitě je dobré vědět, zda je například podpis protistrany na smlouvě platný. A moderní spisová služba nám kromě takového ověření může dovolit smlouvu přímo z aplikace (bez nutnosti použití aplikací třetích stran) také podepsat příslušným certifikátem.

Další, někdy opomíjenou, vlastností je snadná přístupnost k dokumentům a řízení přístupu. Můžeme tak například zpřístupnit faktury a jejich schválení uživatelům, kteří z nějakého důvodu nemají přístup do účetního systému. Pokud je přístup k dokumentům řízen a omezen na oprávněné osoby, minimalizuje to riziko neoprávněného přístupu k citlivým osobním údajům, a to je důležité například z pohledu GDPR.

Mimochodem, z pohledu naplnění GDPR je určitě výhodnější mít informace rozloženy v méně systémech. Spisová služba umožňuje řízení životního cyklu dokumentů, včetně určení doby uchovávání a způsobu a času jejich likvidace (skartace). To je důležitý aspekt z pohledu GDPR na uchování osobních údajů, které stanovuje, že tyto údaje by měly být uchovávány pouze po dobu nezbytnou k dosažení účelu zpracování. Spisová služba může rovněž usnadnit zpracování žádostí od subjektů týkajících se jejich osobních údajů.

To bude asi zbytečně složité a drahé...

Z výše uvedeného vyplývá, že spisová služba je klíčovou součástí správy dokumentů a úspěšného fungování jakékoli organizace. Pro zajištění správného fungování je potřeba nejen kvalifikovaných zaměstnanců, ale také odpovídajících technologií, které umožní zaměstnancům efektivně pracovat. Představili jsme si příklady situací, v nichž je vhodné zapojit do procesů spisovou službu. Nedává však příliš smysl, aby vše obsáhl samotný systém spisové služby. Takový systém by byl zbytečně robustní a drahý. Vhodným řešením je pružný systém spisové služby, který v oblastech kde je to smysluplné umožňuje využití osvědčených a rozšířených nástrojů a technologií, které většina organizací již využívá, případně je má zakoupeny, ale neumí je správně využít. Takové technologie poskytuje například společnost Microsoft prostřednictvím řešení Microsoft 365, který je v mnoha organizacích standardně využíván. Zde je několik tipů, jaké nástroje z tohoto balíku lze využít ve spolupráci se spisovou službou:

- Microsoft SharePoint – platforma pro správu a sdílení dokumentů, která umožňuje vytvářet společné pracovní prostředí pro týmy. V rámci spisové služby může SharePoint sloužit jako centrální úložiště pro agendové dokumenty.
- Microsoft Power Automate – nástroj dříve známý jako Microsoft Flow je nástroj pro automatizaci pracovních postupů. Lze ho využít ve spisové službě pro vytváření automatizovaných toků, které zjednodušují a urychlují procesy správy dokumentů, například notifikace o nových dokumentech, schvalovací procesy nebo správné zatřídění dokumentů.
- Microsoft Teams – Teams je komunikační a kolaborační platforma, která umožňuje týmům komunikovat, sdílet soubory a spolupracovat na dokumentech v reálném čase. V rámci spisové služby může Teams sloužit jako prostředek spolupráce při zpracování agendových dokumentů, jako jsou schvalovací procesy, připomínky nebo diskuze.
- Microsoft Outlook – e-mailový klient, který je součástí Microsoft 365. Může být využit pro správu e-mailové komunikace týkající se agendových dokumentů, jako jsou schvalovací procesy nebo oznámení o změnách dokumentů.
- Microsoft Word, Excel – aplikace pro práci se soubory dokumentů, možnost současné spolupráce více autorů nebo třeba rezervace souborů.

Je to jen teorie nebo „živá“ spisová služba skutečně existuje?

Uvedený přístup naplňuje spisová služba Ordinics, která není jen spisovou službou, ale přináší nový pohled na zpracování dokumentů. Věnuje se nejen uložení dokumentů, ale klade si za cíl automatizovat procesy při jejich zpracování. Plně využívá prostředí Microsoft a je tak plně integrována a kombinovatelná s již existujícími aplikacemi Office od firmy Microsoft. To přináší výhodu efektivity, centralizace, spolupráce a bezpečnosti, což usnadňuje a zlepšuje správu dokumentů v organizaci.

JARVIS – Technologický skok pro moderní státní správu

Jitka Košovanová, Solution Architect, SSP Public, S&T CZ s.r.o.

Elektronická spisová služba JARVIS aplikuje AI v praxi

Spojili jsme dvacetileté zkušenosti ve vývoji, provozování a dodávání spisové služby AthenA s nejnovějším vědeckým výzkumem a vytvořili jsme JARVIS – aplikaci, která pomáhá svému uživateli, přizpůsobuje se jeho požadavkům, udržuje systém, poskytuje přehled či hlídá termíny.

Výzkumný tým S&T CZ do nového softwaru implementoval nejnovější IT technologie, včetně umělé inteligence (AI), vyvinul unikátní metody zpracování a staví na vlastních řešení. Výsledkem je inteligentní služba, kterou lze bezpečně přizpůsobovat individuálním potřebám jednotlivých agend tak, aby za zaměstnance odpracovala maximum rutinních administrativních úkonů.

Modulární architektura umožňuje přizpůsobit prostředí aplikace na míru a dle potřeby ji dále měnit a rozšiřovat. **Ergonomické uživatelské rozhraní** umožňuje nadefinovat viditelnost různých typů informací i zobrazit pouze náhledy ke čtení bez nutnosti otevírat samotné soubory. Jarvis přesněji vyhledává v dokumentech i při zadání nejednoznačného dotazu, zjednodušuje procesy předání, schválení a podepsání dokumentu, automaticky extrahuje data a přesouvá je na další místo zpracování.

Díky **databázové nezávislosti** lze v Jarvisu použít více databázových zdrojů, což uživatelům umožňuje pracovat v různých prostředích nezávisle na technologiích těchto zdrojů.

Zcela novým nástrojem, kterým se Jarvis může pochlubit, je **návrhář workflow**. Pomocí jednoduchého vývojového diagramu lze modelovat vlastní procesy, určit vlastnosti jednotlivých kroků (zasílání e-mailových anotací, změny vlastností komponent, automatické šablonové zpracování), konfigurovat podmínky zpracování dle různých parametrů (když je smlouva od určitého dodavatele, předej ji na definovanou pozici a následně pošli k přednastavenému schválení a podpisu). Vytvořené posloupnosti lze v návrháři verzovat, vracet se k původním variantám a upravovat je. Navíc je možné na jeden dokument aplikovat více procesů, například nejdříve ho předat v rámci organizace a poté ho schvalovat jiným procesem.

V JARVISu jsou integrovány špičkové technologie založené na umělé inteligenci a vlastním vývoji. Uplatňují se mimo jiné v modulu zpracování obrazu, sémantického vyhledávání a automatické anonymizace.

Modul zpracování obrazu převede různorodé dokumenty, jako jsou obrázky, fotografie nebo PDF soubory, na text a následně obsažená data extrahuje a využije v dalším procesu. Například po naskenování faktury je JARVIS schopen ji přečíst a extrahovat potřebná data, která jsou následně automaticky zaslána k dalšímu zpracování. Tímto způsobem je eliminováno manuální vyhledávání a přepisování dat.

Díky **modulu sémantického vyhledávání** odpadá dlouhé pročítání jednotlivých dokumentů, neboť požadavek na hledání se nemusí přesně shodovat s textem obsaženým v dokumentu. JARVIS dokáže rozumět významu textu a hledat informace na základě zadaného výrazu, aniž by byla nutná přesná shoda se slovy obsaženými v dokumentu. To výrazně zjednodušuje a zrychluje vyhledávání.

Dalším užitečným **modulem je automatické anonymizace**, která umí identifikovat a odstranit z dokumentů osobní údaje. Využívá přitom strojového učení a neuronových sítí, které lze „trénovat" i na konkrétní typy dokumentů.

JARVIS poskytuje řešení pro organizace všech velikostí, a to díky své flexibilitě provozu. Je možné ho využívat **jak v cloudu, tak i on-premise**, tedy přímo uvnitř organizace.

JARVIS má jasné ambice posunout zpracování agendy ve státní správě na vyšší úroveň. Elektronická spisová služba nové generace je přívětivá k uživateli, flexibilní, tvárná a spolehlivá.

Od papíru k digitalizaci: Efektivní cesta ke GO Paperless

Bc. Alžběta Křídlová, produktová manažerka, Asseco Solutions, a.s.

Moderní technologie jsou v našem životě stále důležitější. Na chytrá auta, pračky a robotické vysavače jsme si přivykli velmi rychle. Ale v pracovním životě se k technologickým novinkám a automatizaci procesů stavíme stále dost rezervovaně. Proč? Existuje několik důvodů, ale nejpodstatnějším z nich je podle vědeckých studii skutečnost, že se lidé neradi přizpůsobují změnám.

Pokud však chcete ušetřit čas i peníze, je na čase přejít na moderní způsoby práce. Naštěstí již dnes existuje řada nástrojů a technologií, které umožňují digitalizaci firemních procesů. Jedním z těchto nástrojů je GO Paperless.

Koncept bezpapírové kanceláře existuje již celá desetiletí, ale většina organizací stále lpí na svých „papírových zvyklostech". To sebou nese nejen ztracený čas při hledání a třídění informací, tisku, kopírování a skenování dokumentů, ale řada těchto dokumentů obsahuje i osobní či citlivé informace, což znamená, že je nelze jen tak vyhodit. Listinná likvidace je časově i finančně náročnější než ta elektronická.

Fikce nebo realita?

A teď si představte svět GO Paperless, ve kterém byste své firemní procesy svěřili digitálním pomocníkům. O pracovní docházku se postarají moderní docházkové terminály s centrálním řešením i pro více provozů a s přístupem do systému z kteréhokoliv místa na světě. Samozřejmostí je podpora plánování směn, přesčasů a integrace s personálním a mzdovým systémem, včetně výpočtu mezd a graficky ztvárněných reportů. Příjem, třídění, verifikaci, archivací a skartaci dokumentů Vám ohlídá elektronická spisová služba. Vedoucí má k dispozici aktuální i historický přehled o vytíženosti jednotlivých pracovníků. Ekonomické oddělení vám schválí fakturu online na jeden klik a ještě si přečte vaše poznámky umístěné přímo u eDokumentu, které jste mu doplnili přes mobil. Umělá inteligence vás přitom upozorní na anomálie v účetním deníku a sestaví forecast na další období. Pro realizaci projektů, či neočekávaných zakázek si z aplikačního portálu aktivujete přesně takovou aplikaci, kterou potřebujete a ona bude umět automaticky komunikovat s vaším ERP systémem. A možnost, že v digitálním režimu můžete pracovat odkudkoli a kdykoli, je jen drobnou výhodou v řadě dalších. Úplná elektronizace má významný dopad také na bezpečnost vašich dat, protože data uložená v digitální podobě jsou chráněna a šifrována. A pokud svou bezpapírovou kancelář přemístíte na cloudové úložiště, zvýšíte tím nejen úroveň zabezpečení svých dat, ale můžete docílit až 50% úspory personálních a investičních nákladů. Fikce? Nikoli, pouze některé z výhod Paperless kanceláře.

Go paperless by HELIOS

Docházka na jedno pípnutí s docházkovým systém AneT-WebTime.

- Elektronický podpis pracovního listu a digitální přílohy k pracovnímu listu (žádanky, potvrzení...)
- Elektronické schvalování požadavků (např. žádost o dovolenou)
- Elektronické seznamování s plánem a odsouhlasení změn v plánu
- Vše v mobilu na jednom místě, rychle a přehledně

Poznámka k eDokumentu na jeden klik se systémem HELIOS Pantheon pro územní samosprávné celky a větší příspěvkové organizace.

- Systém je zaměřen na ekonomiku organizací.
- Velkou výhodou i přínosem je nastavitelné Workflow, které je výborným pomocníkem pro podporu vnitřních procesů stejně jako hlídání lhůt. Veškerá komunikace je bezpapírová a plně digitalizovaná.
- Pro příspěvkové organizace ekonomika obsahuje moduly Rozpočet, Účetnictví, Výkaznictví, Banka, Pokladna, Faktura vydaná, Faktura došlá.
- Pro územní celky je rozšířen o agendu Místních poplatků a Vymáhání.
- K dispozici jsou Objednávky i Smlouvy, stejně jako modul Finanční kontrola.
- Přímé napojení na spisovou službu SPISKA.

Digitální archivace jedním tlačítkem se spisovou službou Spiska pro komplexní správu vašich dokumentů.

- Elektronická správa Vašich dokumentů, od příjmu dokumentů, přes jejich evidenci, vyřízení, vyhotovení vlastních dokumentů, jejich odeslání, ukládání dokumentů ve spisovně a jejich vyřazování pomocí skartačního řízení.
- Chrání informace obsažené v dokumentech proti zničení nebo ztrátě jejich právních účinků, zajistí orientaci a možnost snadného přístupu k dokumentům.
- Zabezpečí vám správné určení historické hodnoty dokumentů a jejich převzetí k trvalému uložení.

Předcházejte kybernetickým hrozbám a ochraňte svá data na 100 %. Dnešní doba nese s sebou mnoho hrozeb a rizik. Služba phishing směřuje na obranu proti kybernetickým útokům zevnitř. Pomáhá se vzděláním i prověřováním pomocí simulací, následným vyhodnocením i opakovaným mapováním. Není nutná žádná technická podpora, pouze minimální spolupráce na počátku. Služba vede k minimalizaci škod i ohrožení od vlastních uživatelů.

Vykročit k budoucnosti

Digitalizace a paperless ale neznamenají jen úsporu času a peněz, ale také ohleduplnost k životnímu prostředí. Podle studie bylo v roce 2019 na světě vyrobeno přes čtyři biliony listů papíru a až 50% z nich bylo okamžitě vyhozeno. Toto množství odpadu má velký negativní dopad na životní prostředí, protože pro výrobu papíru je potřeba velkého množství vody, energie a dalších zdrojů.

Chcete-li být krok před ostatními a ušetřit si čas i peníze, připojte se ke GO Paperless by HELIOS a vaše firma bude připravena na budoucnost!

Zase to SASE

Pavel Křižanovský, CISCO SYSTEMS (Czech Republic) s.r.o.

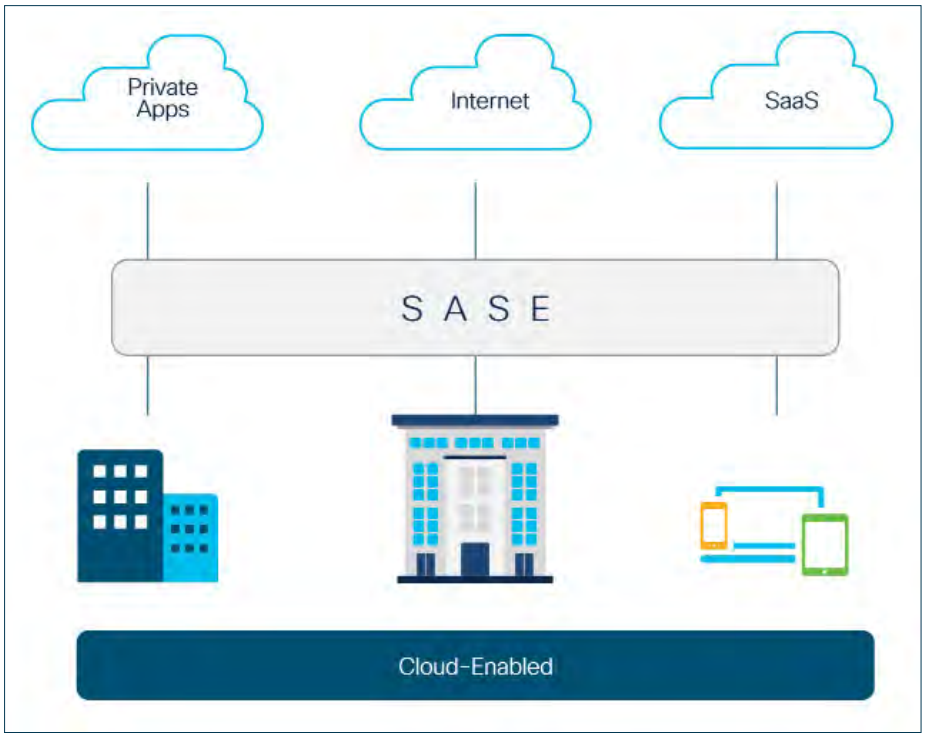
Proč SASE?

Ve světě IT dochází k zásadním změnám. Prudce narůstá práce na dálku a zároveň firmy i veřejné organizace rychle adoptují hybridní cloudové technologie. Zajištění kyberbezpečnosti ve vysoce decentralizovaném prostředí vyžaduje novou filozofii, v níž firmy musí chránit svá data, zaměstnance a aplikace. Odpověď představuje architektura SASE – Secure Access Service Edge.

Co je SASE?

SASE poskytuje bezpečné a bezproblémové připojení k jakékoli aplikaci, přes jakoukoli síť, z jakéhokoli místa nebo zařízení. SASE integruje síťové a bezpečnostní funkce do jednotného cloudového řešení nebo služby. Na rozdíl od tradičních bezpečnostních řešení posouvá bezpečnostní politiky a jejich vynucování blíže ke koncovým uživatelům a aplikacím, které jsou stále více distribuovány. Využívá principů nulové důvěry (Zero Trust) a eliminuje potřebu neustále přenášet data do firemního datového centra, čímž účinně snižuje zatížení sítě a eliminuje úzká místa, a zároveň poskytuje vynikající uživatelskou zkušenost. Jako alternativa k tradičnímu způsobu zabezpečení poskytuje bezpečný přístup od end-to-end, tj. včetně datového centra, vzdálených poboček firem a organizací, mobilních či domácích uživatelů apod.

SASE znamená přechod z aplikačního modelu zaměřeného na datová centra (DC Centric modelu) na model s podporou internetu a cloudu (Cloud-enabled). Od IT týmů to vyžaduje zcela přehodnotit síťovou strategii. Zároveň jim ale pomáhá zajistit bezpečné a bezproblémové prostředí i pro uživatele a aplikace mimo infrastrukturu organizace, kde jsou s vyšší pravděpodobností vystaveni náhodným nebo záměrným bezpečnostním útokům.



Cloudový model SASE spojuje dohromady síťové technologie typu SD-WAN (Software Defined WAN) a cloudová bezpečnostní řešení typu Security Service EDGE (SSE) s využitím principů nulové důvěry (ZTNA – Zero Trust Network Access).

SASE zajišťuje připojení a ochranu uživatelů a aplikací bez ohledu na to, kde se nacházejí nebo hostují, a v konečném důsledku poskytuje lepší, konzistentnější a bezpečnější uživatelské prostředí. Přináší také snížení nákladů a složitosti IT, zlepšení flexibility a výkonu sítě a v konečném důsledku uživatelské zkušenosti.

Cisco SASE (Zase?)

Mnoho firem dnes prezentuje SASE jako zcela zásadní čerstvou novinku.

Zásadní téma SASE zcela jistě představuje, protože vynucuje radikální změny v podnikovém IT, včetně architektury a způsobu zabezpečení. Nicméně se základní definicí SASE přišel Gartner už v roce 2019 a s podrobnější taxonomií včetně dělení na SSE a SD-WAN součásti již v roce 2021. Velká část SASE komponent definovaných Gartnerem už v nějaké podobě existovala dříve. Produkty jako firewall, webová gateway/proxy, zabezpečení DNS či nějakou formu SD-WAN využíváme už řadu let. Dalo by se tedy namítnout, že „zase" někdo vymyslel nový marketingový buzzword, aby přeprodal již existující produkty. Tak to ale není, protože nasazení SASE přináší dvě změny:

1. Jednotlivé technologie jsou použity/provozovány z cloudu formou služby;
2. Komponenty SASE jsou (měly by být) integrovány do jednotné architektury.

Na trhu působí řada dodavatelů, kteří umí (i) z cloudu nabídnout jednu nebo několik SASE komponent. Problém však nastává s bodem č. 2, tedy s kompetencí to celé spojit dohromady. Bez dostatečné integrace jen pokračuje největší bolest dnešních provozovatelů bezpečné IT infrastruktury podniků a organizací: obrovské množství dodavatelů, nástrojů a systémů pro identifikaci problémů a mitigaci bezpečnostních hrozeb.

Cisco je jeden z mála dodavatelů, který nabízí integrované single-vendor SASE řešení. V souladu s Gartnerem zahrnuje Cisco SASE dvě základní součásti:

1. SD-WAN – bezpečné propojení všech lokalit firmy/organizace včetně návaznosti na různé typy cloudových služeb (IaaS, SaaS).
   - Cisco SD-WAN umožňuje end-to-end makro/mikro segmentaci sítě a bezpečný optimalizovaný přístup do cloudu;
   - Vše včetně provisioningu cloudových služeb je součástí workflow v SD-WAN managementu;
   - Řešení umožňuje automatickou optimalizaci cesty do cloudu nejlepší dynamicky určenou cestou (přímý přístup z poboček nebo přes centrálu apod.).
2. SSE (Security Service Edge) integruje pod jednotnou správou následující funkcionality provozované jako služba v cloudu:
   - Ochrana na bázi DNS (DNS layer security);
   - Secure web gateway – bezpečná webová proxy;
   - Next generation cloudový firewall (včetně IPS);
   - Cloud Access Security Broker (CASB) a Data Loss Protection (DLP) systém;
   - Cloud Malware detection, tj. ochrana koncových stanic před malwarem;
   - Zero trust network access (ZTNA) mj. pro bezpečný vzdálený přístup do infrastruktury firmy/organizace (tedy forma cloudového VPN koncentrátoru);
   - Remote Browser Isolation (RBI) – pokročilejší ochrana pro bezpečné prohlížení potenciálně problematických webových stránek;
   - Interactive threat intelligence (Cisco TALOS).

Velká část SSE služeb byla a stále ještě je k dispozici pod značkami Cisco Umbrella a Duo Security, nicméně očekáváme, že v nejbližší době dojde k přejmenování celé této skupiny na Cisco SSE.

Jaké jsou hlavní výhody Cisco SASE?

- Jednotné end-to-end single vendor SASE, tj. integrované řešení celé problematiky;
- Plná automatizace, úplný zero touch deployment (ZTD), integrované workflow zahrnující i provisioning v cloudu;
- Bohaté bezpečnostní funkce podpořené naší security intelligence TALOS;
- Velká a prověřená škálovatelnost (např. >10 tis. poboček v případě SD/WAN, >40 datových center provozujících Cisco SSE služby po světě, jedno z nich je i v Praze);
- Integrovaná analytika a nástroje pro end-to-end vhled i pro provoz cloudových aplikací pro rychlou prevenci, detekci a odstranění provozních i bezpečnostních problémů;
- Otevřený systém s možností integrace i na bázi publikovaných API rozhraní.

Další informace související s Cisco SASE lze najít na https://www.cisco.com/go/sase

Penterep – inovativní platforma pro podporu manuálního penetračního testování

Roman Kümmel, Penterep Security, s.r.o.
Willi Lazarov, Vysoké učení technické v Brně
Zdeněk Martinásek, Vysoké učení technické v Brně

Úvod

Rizika kybernetických útoků na informační systémy státní správy, komerčních firem i běžných koncových uživatelů představují v současnosti reálnou hrozbu, přičemž jejich frekvence se neustále zvyšuje. Dopadem úspěšných útoků jsou většinou finanční ztráty, ale při kybernetických útocích cílených na nemocniční zařízení jimi mohou být i lidské životy [1]. Účinnou obranou je pravidelná realizace a vyhodnocení bezpečnostních penetračních testů. Během nich lze odhalit případné slabiny systémů a aplikací dříve, než je odhalí a zneužijí potencionální útočníci. Potřeba penetračního testování vyplývá také z nové evropské směrnice NIS 2 (Network and Information Security 2), která rozšiřuje počet povinných subjektů a rozsah povinností, jako je zejména nutnost testovat a prokazovat kybernetickou odolnost.

Penetrační testování

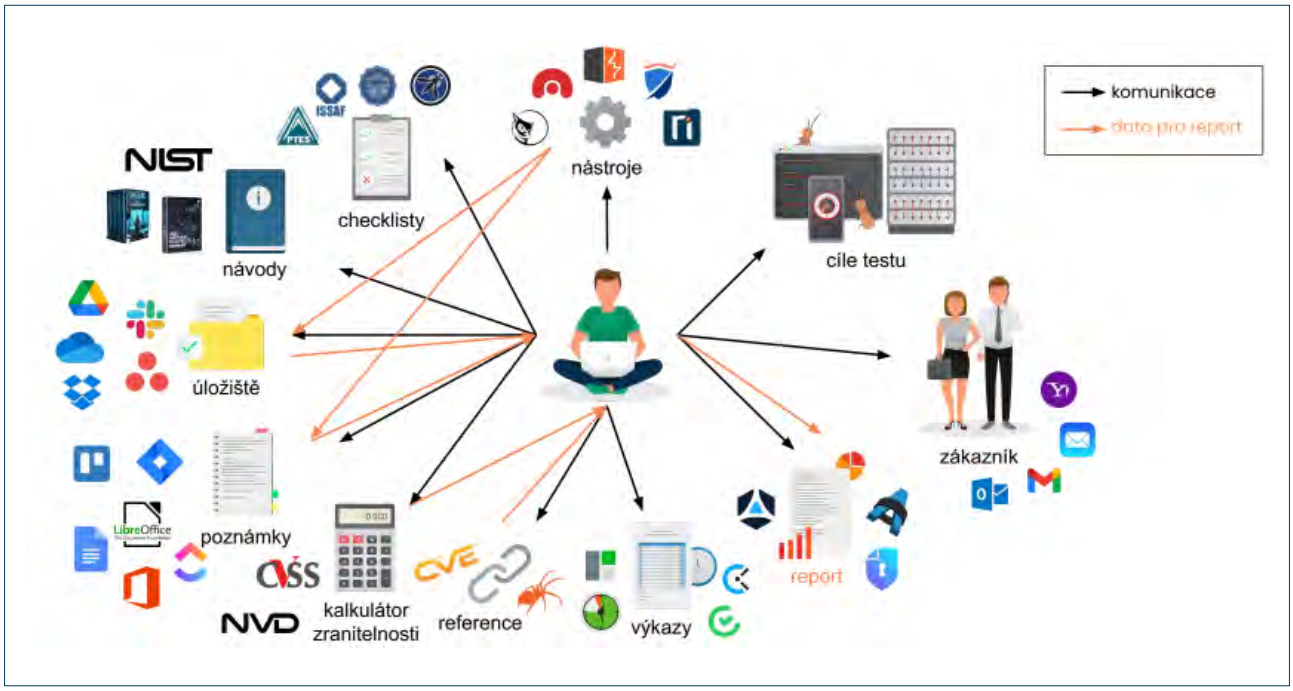
Penetrační testy posuzují úroveň bezpečnosti metodou pokusu o průnik do testovaného systému. Při nalezení zranitelnosti je implementováno bezpečnostní opatření, čímž dochází k průběžnému zvyšování kybernetické odolnosti daného systému. Penetrační testování mohou provádět interní zaměstnanci firem nebo externí specialisté.

Penetrační testování je možné provádět buďto zcela automatizovaně, manuálně nebo pomocí statické analýzy kódu. Plně automatizovaný test je bezesporu nejrychlejším a tím pádem i nejlevnějším řešením. Bohužel při něm ale není možné odhalit všechny zranitelnosti. Například chyby v obchodní logice nemohou být z principu automatickými nástroji odhaleny. Například v případě testování bezpečnosti webových aplikací se účinnost automatů pohybuje pouze kolem 20 % [3]. Statická analýza kódu je speciální variantou automatického testu, během kterého se nevyhledávají zranitelnosti pomocí vstupů do běžící aplikace, ale analýzou samotného zdrojového kódu. Statická analýza může být oproti běžným automatickým nástrojům účinnější, ale opět platí, že některé chyby není možné jejím využitím odhalit. Příkladem neodhalitelných chyb jsou nedostatky v konfiguraci prostředí, ve kterém je aplikace provozována. V případě manuálního penetračního testování je možné se v ideálním případě přiblížit až k 100% účinnosti, což je ovšem vykoupeno časovou náročností a nároky kladenými na zkušenosti penetračního testera [4].

Zatímco pro automatizované testy mají uživatelé na výběr z širokého spektra nejrůznějších nástrojů, na poli manuálního testování příliš velkou softwarovou podporu testeři očekávat nemohou. Testeři často využívají kontrolní seznamy (tzv. checklisty), které jsou definované některým ze standardů, nebo takové, které si sami vytvořili během jejich dlouholeté praxe na základě vlastní zkušenosti. Během manuálního testu si penetrační testeři často píší mnoho poznámek v elektronické, nebo papírové podobě. Popisují jednotlivé nálezy a použité postupy, hodnotí závažnost nálezů, schraňují podklady v podobě snímků obrazovky, videí, úryvků zdrojového kódu, nebo získaných dat. Na konci testu je pak úkolem testera ještě vyhotovení závěrečné zprávy, ve které vedle informací o testovaném prostředí a použitých způsobech musí uvést také detailní popis každého nálezu včetně ohodnocení jeho závažnosti, možných dopadů při zneužití a doporučení k nápravě. Tvorbou závěrečné zprávy stráví tester mnohdy stejně času, jako samotným testováním [5].

Z výše popsaných faktů je zřejmé, že kritickými problémy manuálního testu jsou velká závislost výsledku na zkušenostech, znalostech a inteligenci testera, dále jeho závislost na časové kapacitě, použitých nástrojích a metodologii. Díky tomu je testování realizováno často nesystematicky, zdlouhavě a chaoticky bez vhodné možnosti sdílení výsledků v pracovním týmu. Pro realizaci

komplexního bezpečnostního testu je ovšem nezbytné postupovat systematicky, kombinovat automatické nástroje a náročné manuální testy (viz obr. 1). V současnosti existuje velké množství dílčích, jednoúčelových nástrojů, které mohou testeři při své práci využívat. Na trhu ovšem neexistuje žádný nástroj, který by manuální testování pojímal komplexně. Tedy takový, který by slučoval funkcionalitu těchto nástrojů, propojoval manuální testování s automatizovanými nástroji a prováděl by penetračního testera při práci krok za krokem.



Obr. 1. Problematika penetračního testování

Platforma Penterep

V rámci účinné spolupráce odborníků na kybernetickou bezpečnost z **Ústavu telekomunikací VUT v Brně** a předním expertem na penetrační testování webových aplikací **Romanem Kümmelem** vznikla platforma **Penterep**[1], která si klade za cíl v maximální možné míře zjednodušit a zpřehlednit práci penetračních testerů. Jedním z přínosů platformy je přiblížit možnost interního testování běžným uživatelům, kteří mají pouze základní znalosti o penetračním testování. **Penterep** je inovativní platforma, která provádí penetračního testera jednotlivými kontrolními seznamy tak, aby bylo vždy zřejmé, jaký test se má právě vykonat. Tester má u každého testu k dispozici také podrobný návod, jak daný test realizovat, díky čemuž je možné do testování **zapojit i méně zkušené začínající testery**, kteří se během práce současně vzdělávají. Případné nálezy jsou v platformě evidovány jako výsledky jednotlivých testů včetně hodnocení závažnosti a případných příloh. Platforma poskytuje **rozsáhlou znalostní bázi**, ve které jsou již všechny zranitelnosti důkladně popsány. Testerům díky tomu stačí konkrétní zranitelnost pouze vybrat ze seznamu. Efektivní přístup k realizaci penetračních testů za pomoci platformy Penterep je zobrazeno na obr. 2.

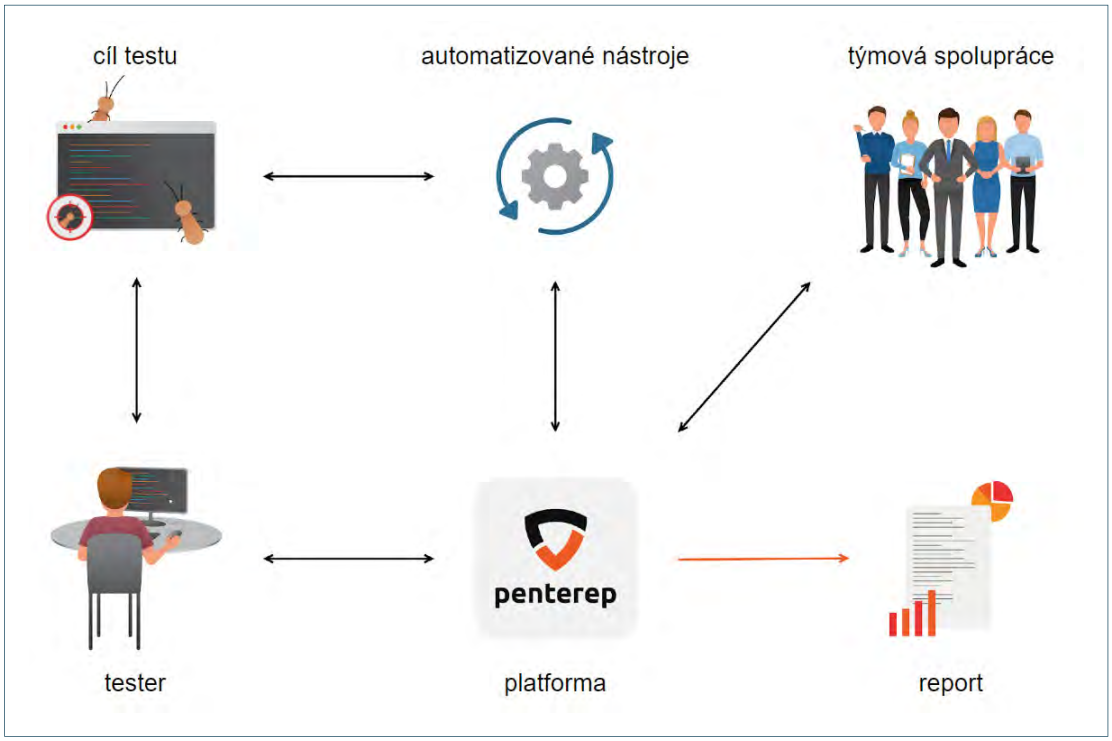
Na testování cílového prostředí může pracovat současně i více testerů, aniž by některé součásti zůstaly neotestovány, nebo aby se práce testerů opakovala. Každý člen týmu má totiž okamžitý přehled o tom, které testy jsou již hotové, a které na provedení teprve čekají. Systém oprávnění umožňuje přidělit přístup k jednotlivým testovaným součástem konkrétním testerům. Do týmu lze přidat také IT (Informační technologie) pracovníky nebo vývojáře zodpovědné za bezpečnost testovaného prostředí. Tito

1 Projekt aplikovaného výzkumu byl spolufinancován se státní podporou Technologické agentury ČR v rámci Programu ZÉTA 4, reg. č. TJ04000456.

pracovníci díky tomu mohou v reálném čase nalezené zranitelnosti komentovat, nebo mohou rovnou implementovat protiopatření, která předají testerům zpět k přezkoumání. Mimo to mají testeři k dispozici také možnost volat přímo z platformy Penterep skripty pro automatizované testování, přičemž výsledky těchto skriptů jsou po skončení práce předány platformě, kde jsou automaticky zaevidovány.

Obr. 2. Problematika penetračního testování

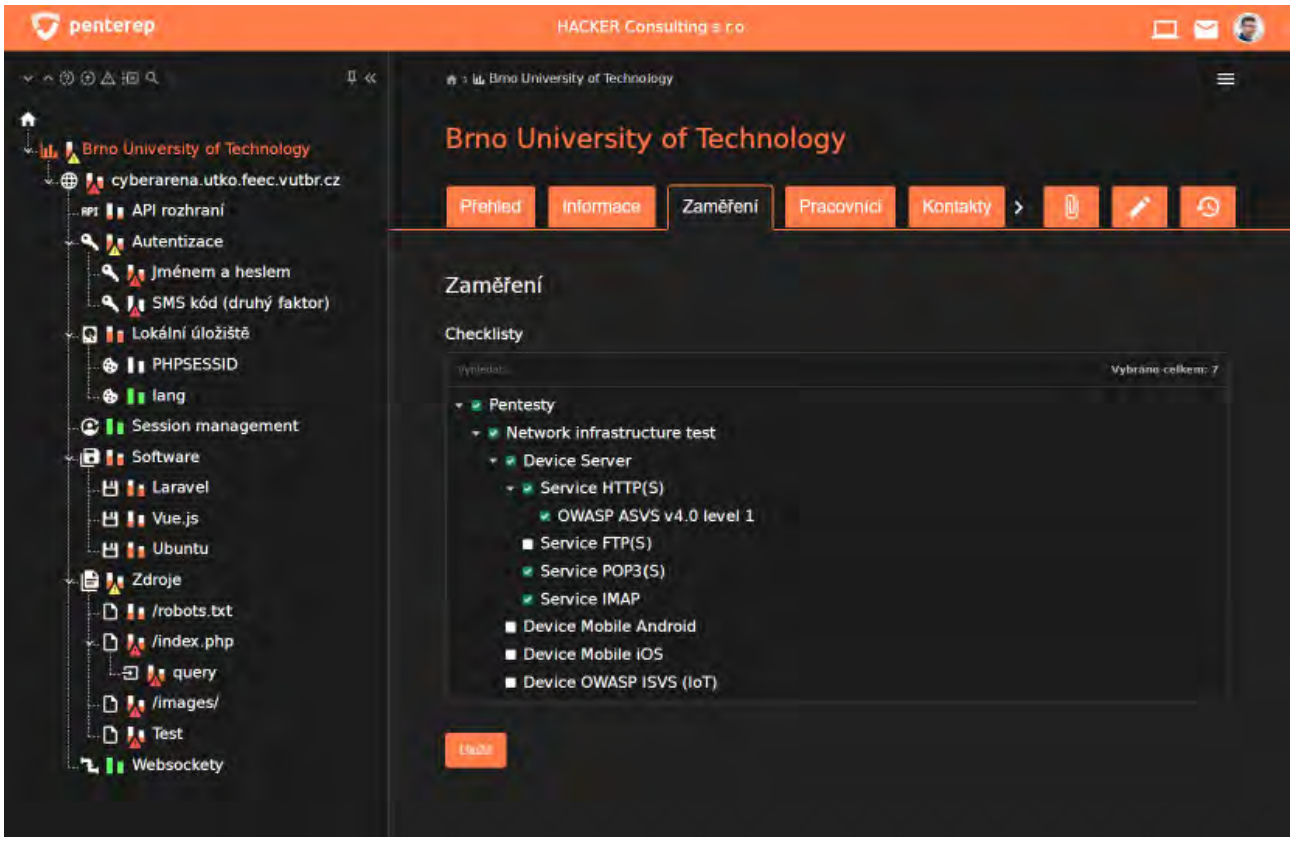
Po ukončení testování vyhotoví platforma **Penterep** zcela **automaticky závěrečnou zprávu** (report) s uvedením všech standardních náležitostí a soupisem všech odhalených zranitelností včetně jejich ohodnocení, doporučením k nápravě atd. Díky znalostní bázi je do reportu k jednotlivým nálezům doplněno také provázání na reference, popis relevantních útoků a další informace. K reportu jsou automaticky přiloženy také přílohy, které testeři vložili během testování. Celý proces užití platformy Penterep je znázorněn na obr. 3.



Obr. 3. Schéma užití platformy Penterep

Co vše lze s platformou Penterep testovat

Nástroj **Penterep** se nezaměřuje na testování pouze jedné konkrétní specifické oblasti. Jedná se o platformu pro penetrační testování, která je díky modulárním kontrolním seznamům snadno rozšiřitelná na libovolnou oblast, jako je např. testování webových[2] a mobilních aplikací, forenzní analýzu, síťovou infrastrukturu, aplikačního serveru, síťových služeb[3], OSINT (Open Source Intelligence) aj. (viz obr. 4). Implementované kontrolní seznamy přitom reflektují světově uznávané standardy, mezi které patří například OWASP (Open Web Application Security Project) nebo NIST (National Institute of Standards and Technology). Na tvorbě těchto kontrolních seznamů se **aktivně podílí odborníci z praxe**, a to **penetrační testeři z NÚKIB** a **bezpečnostní specialisté ze společnosti ATS-TELCOM PRAHA a.s.** Penterep nabídne také pomoc při nutnosti testování a prokazování kybernetické odolnosti, která plyne z nové evropské směrnice NIS 2. Platforma je k dispozici ve formě cloudového software jako služba (SaaS – Software as a Service), nebo je možné platformu nasadit na vlastní server (on-premise řešení).



Obr. 4. Výběr kontrolních seznamů v platformě Penterep

Závěr

Díky inovativním vlastnostem platformy Penterep je s její pomocí možné realizovat bezpečnostní testy nejen kvalitněji, ale i mnohem efektivněji, než by tomu bylo bez jejího použití. Uživatelé platformy mohou navíc ušetřit nemalé finanční prostředky, které by jinak museli investovat do nákupu licencí mnoha jednoúčelových nástrojů, nebo do vzdělávání pracovníků.

2 Kontrolní seznamy jsou výsledky projektu TJ04000456, který byl spolufinancován se státní podporou Technologické agentury ČR v rámci Programu ZÉTA 4.

3 Tyto kontrolní seznamy jsou plánované výsledky projektu VK01030019, který je aktuálně v řešení a spolufinancován se státní podporou Ministerstva vnitra ČR v rámci Programu OPSEC.

Zdroje

[1] CHOI, Sung J.; JOHNSON, M. Eric; LEHMANN, Christoph U. Data breach remediation efforts and their implications for hospital quality. Health services research, 2019, 54.5: 971-980.

[2] SHAH, S.; MEHTRE, B. M.; CHU, B. T. B.; JONES, M. An overview of vulnerability assessment and penetration testing techniques. In Journal of Computer Virology and Hacking Techniques. [online]. 2015, 11(1), 27–49 [cit. 2021-10-10]. ISSN 2263-8733.

[3] MIRJALILI, Mahin; NOWROOZI, Alireza; ALIDOOSTI, Mitra. A survey on web penetration test. Advances in Computer Science: an International Journal, 2014, 3.6: 107-121.

[4] STEFINKO, Yaroslav; PISKOZUB, Andrian; BANAKH, Roman. Manual and automated penetration testing. Benefits and drawbacks. Modern tendency. In: 2016 13th international conference on modern problems of radio engineering, telecommunications and computer science (TCSET). IEEE, 2016. p. 488-491.

[5] BACUDIO, A. G.; YUAN, X. A.; CHU, B. T. B.; JONES, M. An Overview of Penetration Testing. In International Journal of Network Security & Its Applications. 2011, 3(6), 19–38. ISSN 2324-8157.

Co se změnilo za rok v tvorbě elektronických dokumentů?

Mgr. Tomáš Lechner, Ph.D.,
Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra práva

Úvod

Dokumentový přístup je základem současného způsobu úřadování aplikovaného již několik století. Ačkoliv elektronizace otevírá i další možnost, např. v transakčním přístupu, je stále dokumentační hodnota dokumentů schopných zaznamenat právní stav v čase včetně záznamu (dokladu) projevu vůle stěžejní pro výkon veřejné správy. V případě listinných dokumentů je zcela přirozená snaha autorů vytvářet je tak, aby měly určité, byť mnohdy i nepsané, kvality. Kvalita listinných dokumentů zahrnuje jak technickou stránku, tedy použitý druh papíru a inkoustu, jakým je na něj zaznamenáván obsah, tak stránku obsahovou. V případě tvorby elektronických dokumentů jsou nároky na obsahovou stránku zcela shodné s dokumenty listinnými. Vyjadřuje se k nim např. § 16 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ale také § 18 či § 68 až 69 správního řádu, popř. další ustanovení dalších procesně právních předpisů. Zbývá však stále ne příliš uspokojivě řešená stránka technické kvality.

Technická kvalita elektronických dokumentů má dvě složky. První je volba datového formátu, což je způsob kódování komponenty, který zajišťuje uložení dokumentu nebo jeho části (částí) pro účely zpracování výpočetní technikou a jeho znázornění (definice převzatá z Národního standardu pro elektronické systémy spisové služby [2]). Druhou je volba datového nosiče, kde je dokument uchováván. V rámci tohoto příspěvku se soustředíme na první složku, neboť primárně představuje zásadnější výzvu. Pokud nejsou vytvořena kvalitní data, je pak úplně jedno, kde je budeme uchovávat. Prezentovaný výzkum dále navazuje na příspěvek [1] a srovnává aktuální stav se stavem analyzovaným v roce 2022.

Výstupní datové formáty

Elektronickým dokumentem se podle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, známého pod zkratkou eIDAS, rozumí jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka. Naproti tomu obecně dokumentem se podle § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě, rozumí každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena. K tomu dále platí, že veřejnoprávní původci, kteří vykonávají spisovou službu v elektronické podobě (což v nepříliš vzdálené budoucnosti budou vlastně všichni veřejnoprávní původci, jak nastavil zákon č. 261/2021 Sb., o další elektronizaci postupů orgánů veřejné moci), a tedy ti, kteří primárně tvoří prvopisy dokumentů právě v elektronické podobě (§ 16 odst. 3 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby), musí zajistit, aby tyto dokumenty vystupovaly ze spisové služby ve výstupním datovém formátu podle § 23 odst. 1 písm. a) cit. vyhlášky č. 259/2012 Sb.

Je jistě trochu škoda, že na užití výstupních datových formátů se pohlíží jako na něco specifického jen pro výkon spisové služby. Je to obdobné, jako kdyby platilo, že listinný dokument evidovaný ve spisové službě musí být vytištěn na kvalitním papíře způsobem, který zaručí jeho trvanlivost, ale listinný dokument, který není evidován ve spisové službě, může být načmárán obyčejnou tužkou na útržek toaletního papíru. To samozřejmě tak není a nikdo se při tvorbě listinných dokumentů neohlíží na to, zda tento dokument je evidován ve spisové službě jako základní evidenční pomůcce, nebo zda je evidován třeba v samostatné evidenci dokumentů. Tvorba listinných dokumentů je přirozená a zavedená dlouhodobou praxí. Stejně tak by se ale mělo posunout vnímání v oblasti tvorby elektronických dokumentů, kde tím primárním základem je volba takových datových formátů, které:

- budou mít perspektivu dlouhodobé čitelnosti,
- budou dodržovat zásadu technologické neutrality, vyžadovanou mimo jiné zákonem č. 12/2020 Sb., o právu na digitální služby, a
- budou schopné adekvátně zaznamenat důkaz projevu vůle v podobě kvalifikovaného elektronického podpisu.

Pro statické textové a statické kombinované textové a obrazové dokumenty je takovým formátem PDF/A-2 a vyšší. jejichž základní rozbor lze najít např. v [3]. Vyhláška č. 259/2012 Sb. k tomu dodává, že verze PDF/A-3 a vyšší je výstupním datovým formátem statických textových dokumentů a statických kombinovaných textových a obrazových dokumentů, neobsahuje-li dokument v datovém formátu, který není výstupním datovým formátem, a dokument obsahující další dokumenty.

Samozřejmě, že ne všechny elektronické dokumenty musí být statické, a proto jsou definovány i další výstupní datové formáty. Jejich celkový přehled podle § 23 vyhlášky č. 259/2012 Sb. je následující:

- Výstupním datovým formátem statických textových dokumentů a statických kombinovaných textových a obrazových dokumentů datový formát Portable Document Format for the Long-term Archiving (PDF/A, ISO 19005).
- Výstupním datovým formátem statických obrazových dokumentů je buď datový formát Portable Network Graphics (PNG, ISO/IEC 15948), nebo datový formát Tagged Image File Format (TIF/TIFF, revize 6 - nekomprimovaný), anebo datový formát Joint Photographic Experts Group File Interchange Format (JPEG/JFIF, ISO/IEC 10918).
- Výstupním datovým formátem dynamických obrazových dokumentů je buď datový formát Graphics Interchange Format (GIF), nebo některý z datových formátů MPEG. Konkrétně může být použit buď datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 1 (MPEG-1, ISO/IEC 11172), nebo datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 2 (MPEG-2, ISO/IEC 13818), anebo datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 4 (MPEG-4, ISO/IEC 14496).
- Výstupním datovým formátem zvukových dokumentů je datový formát umožňující uložení komprimovaných dat kódovaných podle standardu MPEG-1 Audio Layer II nebo MPEG-2 Audio Layer II (MP2), nebo datový formát umožňující uložení komprimovaných dat kódovaných podle standardu MPEG-1 Audio Layer III nebo MPEG-2 Audio Layer III (MP3), a konečně lze také použít datový formát Waveform audio format (WAV), modulace Pulse-code modulation (PCM).
- Výstupním datovým formátem pro databáze a datové věty je datový formát Extensible Markup Language Document (XML), kde součástí předávaného dokumentu v datovém formátu XML je popis jeho struktury pomocí schématu XML nebo Document Type Definition (DTD), o kterém veřejnoprávní původce vede dokumentaci.
- Výstupním datovým formátem pro účetní záznamy v elektronické podobě, jejichž obsahem je elektronická faktura, je datový formát Information System Document (ISDOC) verze 5.2 a vyšší nebo datový formát, který je v souladu s evropskou normou pro sémantický datový model základních prvků elektronické faktury a syntaxí podle směrnice Evropského parlamentu a Rady č. 2014/55/EU, o elektronické fakturaci při zadávání veřejných zakázek.
- Výstupním datovým formátem metadat, jimiž jsou opatřovány dokumenty v elektronickém systému spisové služby, je datový formát Extensible Markup Language Document (XML) podle schématu XML pro výměnu dokumentů a jejich metadat mezi elektronickým systémem spisové služby stanoveného národním standardem nebo datový formát Extensible Markup Language Document (XML) podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem, který obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem.

Postup analýzy

V minulém roce jsme analyzovali období měsíce března aktuálního roku 2022 [1]. Letos jsme z důvodu větší průkaznosti a delšímu přípravnému období vzali celý první kvartál rok 2023. Stejně jako minule jsme oslovili několik veřejnoprávních původců vedoucích spisovou službu v elektronické podobě, avšak nikoliv s dotazem na jimi vytvářené dokumenty, ale zajímala nás statistika datových formátů přijatých jejich podatelnami od jiných orgánů veřejné moci. Tím jsme byli schopni i z poměrně

mála statistických souborů (4 městských a obecních úřadů) provést analýzu dokumentů vytvořených více než 200 (tedy o několik jednotek více než v loňské analýze [1]) různými orgány veřejné moci, což zahrnuje přibližně 1 % všech stávajících orgánů veřejné moci.

Do analýzy vstoupily statistické výstupy z elektronických systémů spisových služeb vytvořené podle požadavku 2.1.15 a 8.2.3 písm. b) národního standardu pro elektronické systémy spisové služby [2]. Vybrány byly pouze ty komponenty dokumentů, které byly přijaty z datové schránky jiného orgánu veřejné moci, aby se jednak odstínily výstupy převodu podle zákona č. 499/2004 Sb., které provádí přímo původce, a jednak, aby nebyla statistika zatížena dokumenty přijatými od subjektů, jichž se povinnost tvořit elektronické dokumenty ve výstupním datovém formátu netýká.

Celkem bylo analyzováno 2834 komponent dokumentů, které byly přijaty podatelnami oslovených původců v období od 1. ledna do 31. března 2023. Původ dokumentů byl ověřen dle identifikátoru datové schránky zkontrolovaný vůči otevřeným datům obsahujícím seznam datových schránek orgánů veřejné moci a dostupný na <https://www.mojedatovaschranka.cz/sds/datafile?format=xml&service=seznam_ds_ovm> [3]. Díky této kontrole bylo navíc možné kategorizovat tyto datové schránky, přičemž byly zvoleny následující skupiny (shodné s loňskou analýzou [1]):

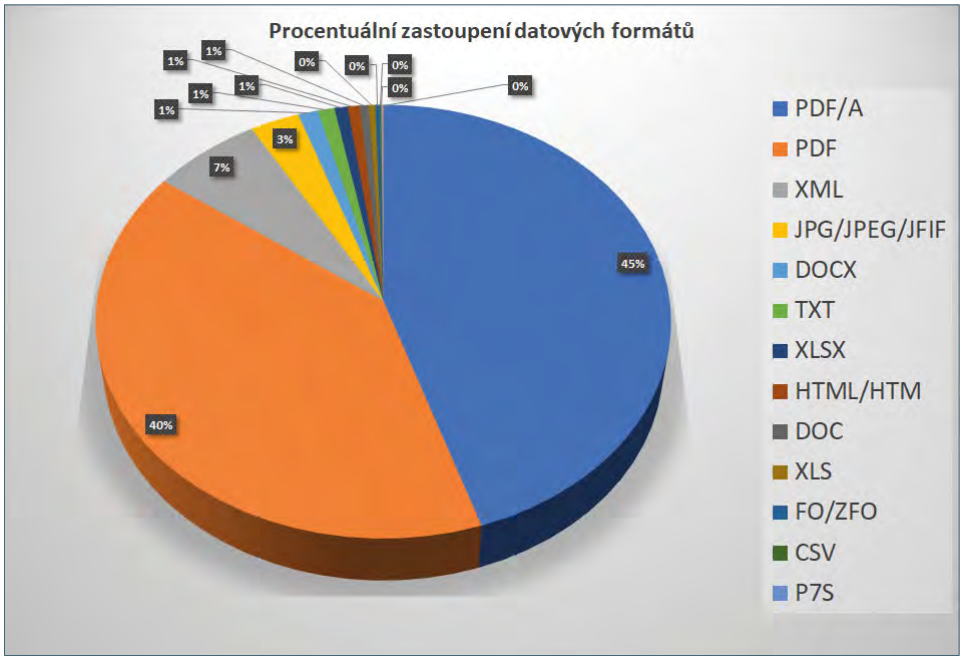
- Ministerstva
- Soudy
- Policie
- Městské, obecní a krajské úřady, úřady městských částí a magistráty (municipality)
- Školy
- Ostatní (jiná OVM, která nespadají do žádné z výše uvedených kategorií, jako např. státní fondy, různé agentury apod.)

Výsledky

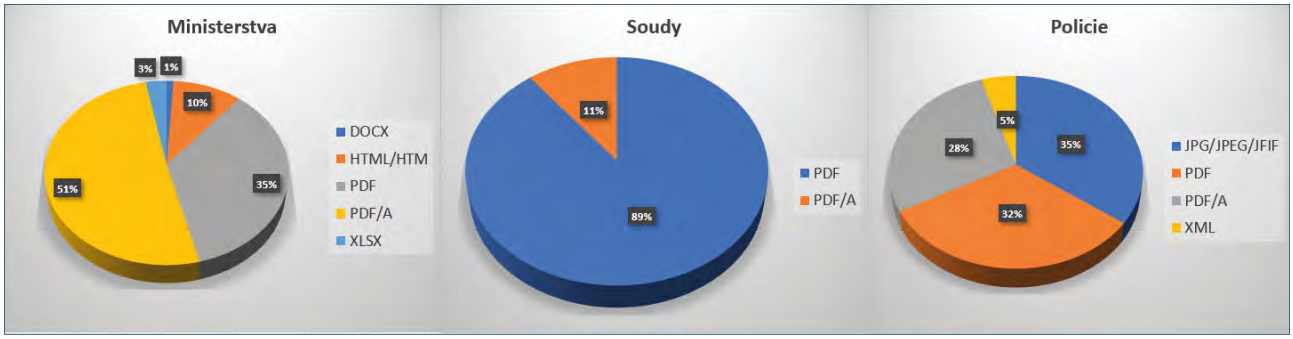
Obr. 1 ukazuje aktuální četnost jednotlivých datových formátů přes všechny kategorie orgánů veřejné moci. Z grafu je zřejmé, že nejčetnějším datovým formátem je PDF/A, jehož procentuální zastoupení je 45 %. Ale nevýstupní datový formát PDF má bohužel také vysokou četnost, a to hned na druhém místě v celkové četnosti 40 %.

Obr. 2. pak ukazuje četnost jednotlivých datových formátů pro kategorie ministerstva, soudy a policie. Pro ministerstva je nejčetnějším formátem PDF/A přibližně v 51 %, pro soudy bohužel nevýstupní datový formát PDF, a to dokonce v 89 % případů a pro polici obrazová dokumentace ve formátu JPG v 35 %.

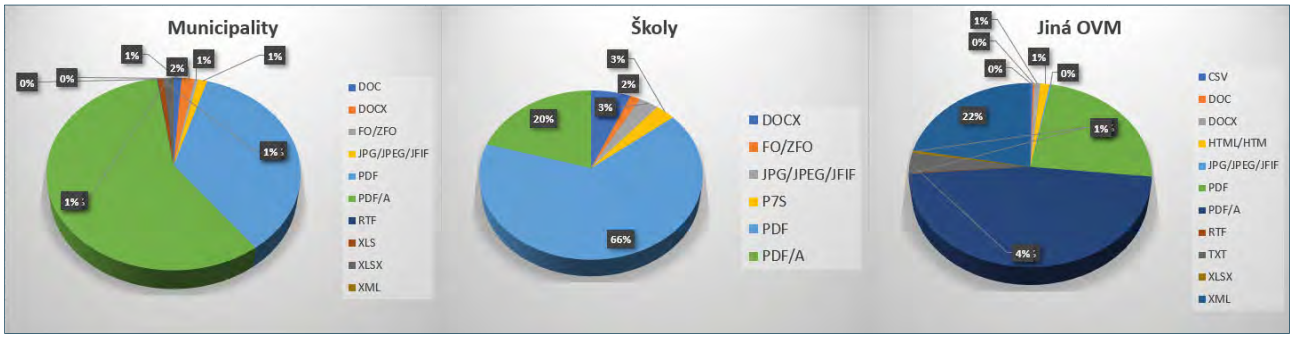
Obr. 3 následně prezentuje tutéž statistiku, ale pro kategorie municipality, školy a ostatní. Od krajů, měst a obcí nejčastěji chodí komponenty v datovém formátu PDF/A, a to v 58 % případů, od škol je to opět bohužel nevýstupní datový formát PDF ve dvou třetinách všech případů, a od jiných OVM přichází nejčastěji v přibližně 47 % výstupní datový formát PDF/A.



Obr. 1: Procentuální zastoupení datových formátů přijatých ode všech orgánů veřejné moci



Obr. 2: Procentuální zastoupení datových formátů pro kategorie OVM ministerstva, soudy a policie.



Obr. 3: Procentuální zastoupení datových formátů pro kategorie OVM municipality, školy a jiná OVM (ostatní).

Diskuse

Základní statistika přijatých datových formátů z datových schránek OVM na Obr. 1 ukazuje, že se mezi těmito datovými formáty vyskytují jak výstupní, tak také nevýstupní formáty. Výstupní datové formáty (PDF/A, XML, JPG) tvoří dohromady 54,7 % všech přijatých komponent. Zbytek, tedy 45,3 % všech přijatých komponent bylo v nevýstupním datovém formátu. Jsme si vědomi ustanovení § 23 odst. 9 vyhlášky č. 259/2012 Sb., které připouští použití nevýstupního datového formátu v případě, kdy je současně použit také výstupní datový formát, ale toto ustanovení nemůže vysvětlit stále tak velké procentuální zastoupení nevýstupních datových formátů. Minimálně u datového formátu PDF nedává současné použití s výstupním datovým formátem smysl.

Datový formát	Procentní zastoupení 2022	Procetní zastoupení v roce 2023	Progres
PDF/A	32,7%	45,0%	12,3%
PDF	47,8%	40,0%	-7,8%
XML	9,4%	6,7%	-2,7%
JPG/JPEG/JFIF	4,2%	3,0%	-1,2%
DOCX	1,5%	1,2%	-0,2%
TXT	0,8%	1,0%	0,3%
XLSX	0,1%	0,8%	0,7%
HTML/HTM	2,0%	0,7%	-1,2%
DOC	0,4%	0,6%	0,2%
XLS	0,1%	0,4%	0,3%
FO/ZFO	0,9%	0,2%	-0,6%
CSV	0,2%	0,1%	-0,1%
P7S/TST	0,1%	0,1%	0,0%
RTF	0,1%	0,1%	0,0%

Tab. 1: Vývoj procentního zastoupení datových formátů

V Tab. 1 jsou hodnoty procentního zastoupení jednotlivých datových formátů v roce 2023 srovnány s výsledky z počátku roku 2022, které byly analyzovány v [1]. Zeleně jsou zvýrazněny řádky s nárůstem a červeně s poklesem procentního zastoupení. Z hlediska výstupního datového formátu PDF/A je patrný příznivý trend nárůstu o celých 12,3 procentního bodu. Nejvýraznější pokles byl zaznamenán u nevýstupního datového formátu PDF, což je opět příznivý výsledek, protože právě tento formát nemá ve srovnání s PDF/A užitné opodstatnění, na rozdíl třeba od tabulkových formátů XLSX nebo CSV, pro jejich použití může být praktický důvod, který by měl být samozřejmě doplněn aplikací výše citovaného ustanovení § 23 odst. 9 vyhlášky č. 259/2012 Sb.

Stěžejní pro naši diskusi je však zastoupení výstupních a nevýstupních datových formátů. Celkový přehled identifikovaných formátů jednoznačně ukazuje, že mezi všemi sledovanými OVM jasně převládají statické textové dokumenty a statické kombinované textové a obrazové dokumenty. Nebyl identifikován žádný datový formát pro dynamické obrazové nebo zvukové dokumenty. Srovnání procentního zastoupení výstupních (z uvedených případů PDF/A, XML a JPG) a ostatních nevýstupních datových formátů je v Tab. 2.

Celkově je patrný za uplynulý rok určitý nárust užití výstupních datových formátů, což je jistě velmi chvályhodné. Avšak uvedená změna pořád ještě nedosahuje kvalit, které by elektronické dokumenty produkované veřejnou správou měly mít.

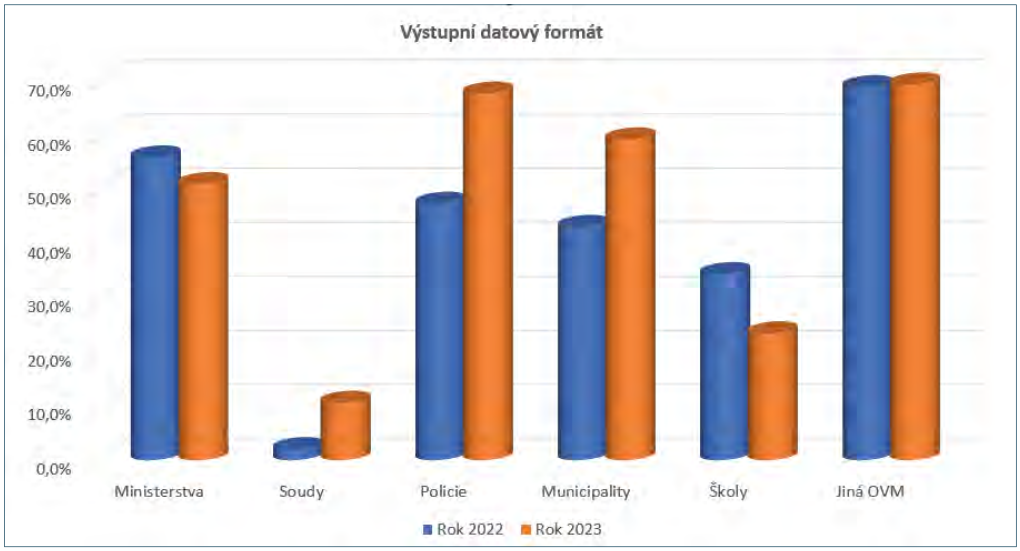
Datový formát	Procentní zastoupení 2022	Procetní zastoupení v roce 2023	Progres
Výstupní datové formáty	46,3%	54,7%	8,4%
Nevýstupní datové formáty	53,7%	45,3%	-8,4%

Tab. 2: Vývoj výstupních a nevýstupních datových formátů.

Podívejme se ještě na srovnání užití výstupních a nevýstupních datových formátů jednotlivými kategoriemi orgánů veřejné moci. Výsledky jsou znázorněny na Obr. 4. V případě ministerstev a škol je patrné mírné zhoršení situace, naproti tomu soudy, policie a municipality produkují oproti loňskému roku více kvalitních elektronických dokumentů.

Prvenství v užití výstupních datových formátů si stále udržují jiná OVM, která nespadají do žádné z ostatních uvedených specifických kategorií. Tyto subjekty posílají výstupní datové formáty v téměř 70 % všech případů. Avšak druhé místo, které ještě vloni patřilo ministerstvům, letos obsadila policie. Navíc, její nárůst kvality dokumentů ve smyslu užívání výstupních datových formátů je v absolutním vyjádření nejvyšší, více než 20 procentních bodů. Druhý v pořadí, kdo se nejvíce zlepšil, jsou municipality. U nich bylo zjištěno zkvalitnění ve výši 16,2 procentního bodu, a celkově již produkují téměř 60 % dokumentů ve výstupních datových formátech.

Zlepšení je patrné také v případech soudů, nicméně pořád vytvářejí pouze přibližně 11 % dokumentů ve výstupních datových formátech, takže jsou stále nejhorší skupinou orgánů veřejné moci z tohoto úhlu pohledu. Předposlední místo patří školám, které se za poslední rok nejvíce zhoršily o téměř 11 procentních bodů, takže více než tři čtvrtiny jimi vytvořených dokumentů nejsou ve výstupních datových formátech, a to navíc tím, že vytvářejí pouze PDF namísto správného PDF/A.



Obr. 4: Srovnání procentního zastoupení výstupních datových formátů pro jednotlivé kategorie OVM v letech 2022 a 2023.

Shrnutí

Z námi provedené analýzy vyplynulo, že oproti loňskému roku došlo celkově ve veřejné správě k mírnému zlepšení z hlediska užívaných datových formátů a uvědomění si faktu, že výstupní datové formáty nejsou zbytečný výmysl specifický jen pro spisovou službu, ale že jsou základem technické kvality tvorby dokumentů, zejména veřejných listin v elektronické podobě. Nicméně

pořád ještě necelá polovina dokumentů vytvářených orgány veřejné moci je v nevýstupních datových formátech. Největší nedostatky přetrvávají v použití PDF namísto PDF/A, což nemůže být připsáno např. potřebě vyplňování tabulek či jiných specifických souvislostí, ale jednoznačně ukazuje na nedostatky v tvorbě dokumentů.

Pokud si uvědomíme, že každý orgán veřejné moci má při uložení dokumentu povinnost převést dokument do výstupního datového formátu, přičemž ověřovací doložka musí být kromě podepsání či pečetění též označena kvalifikovaným elektronickým časovým razítkem, za jehož vydání platí orgány veřejné moci poskytovatelům kvalifikovaných služeb vytvářejících důvěru pro elektronické transakce, je zřejmé, že tato nekvalita tvorby dokumentů má nejen omezující dopady na adresáty dokumentů, ale přináší také nemalé náklady vlastní veřejné správě.

Z hlediska detailní analýzy pro vybrané kategorie orgánů veřejné moci lze pochválit zejména policii a municipality, kde došlo k výraznému zlepšení. Zlepšení bylo zjištěno také v případě soudů, ale protože tyto subjekty patří trvale k nejhorším z hlediska kvality vytvářených elektronických dokumentů, je výsledek sice optimistický, ale stále výrazně nedostatečný. Překvapivé bylo, že u ministerstev a škol došlo dokonce ke zhoršení situace, a v případě škol dokonce výraznému.

Je tedy třeba i nadále sledovat kvalitu vytvářených elektronických dokumentů a soustředit se na osvětu v této oblasti, aby se zbránilo zbytečným výdajům spojeným s nápravou nevhodně vytvářených dokumentů a aby se celková kvalita elektronických dokumentů vytvářených veřejnou správou dále po technické stránce zlepšovala.

Literatura

[1] LECHNER, T. Jak se (ne)využívají výstupní datové formáty? In: PÁNKOVÁ, K. (ed.) Sborník 24. konference ISSS [online]. Hradec Králové, 16.05.2022 – 17.05.2022. Praha: Triada, 2022, s. 28–33. eISBN 978-80-907164-4-5. Dostupné z: https://www.isss.cz/archiv/2022/download/isss2022-sbornik.pdf.

[2] MINISTERSTVO VNITRA. Národní standard pro elektronické systémy spisové služby. 4. verze. Věstník Ministerstva vnitra, částka 57/2017.

[3] KUNT, M., LECHNER, T. Spisová služba. 3. aktualizované vyd. Praha: Leges, 2022. 412 s. Praktik. ISBN 978-80-7502-616-3.

[4] Seznam datových schránek orgánů veřejné moci publikovaný jako OpenData a dostupný na adrese <https://www.mojedatovaschranka.cz/sds/datafile?format=xml&service=seznam_ds_ovm>. Citace 15. 4. 2023.

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/14/2022.

Novinky v inkoustovém kancelářském tisku

Martin Lucký, Pre/Post Sales Specialist, Epson Europe CZ & SK

Společnost Epson pokračuje v přechodu k čistě inkoustovému portfoliu kancelářských tiskáren. Na konci loňského roku uvedla tiskárnu formátu A4 WorkForce WF-C5390 a multifunkční zařízení WF-C5890. Tyto zařízení směřují do malých a domácích kanceláří a představují alternativu menších laserových tiskáren s rychlostí tisku 25 A4 stran za minutu. Aktuální novinkou v produktové řadě představují kompaktní multifunkční tiskárny AM-C4000/C5000/C6000, které nabízí kancelářský tisk do formátu A3 rychlostí 40/50/60 stan A4/min. Tyto zařízení doplňují řadu tiskáren Workforce a Enterprise, která tak nabízí rychlosti tisku od 20 do 100 A4 stran/min.

Inkoustové tiskárny Epson používají osvědčené piezoelektrické hlavy PrecisionCore navržené na celou životnost zařízení bez nutnosti výměny. Při tisku se nevytváří škodlivý ozón a množství prachových částic je výrazně nižší než u laserových tiskáren, což umožňuje nasazení nejen v kancelářích, ale i v čistých provozech jako jsou laboratoře či nemocnice. Tiskový proces je studený, tedy Heat-Free, neohřívá okolní prostředí a vyniká nízkou spotřebou energie. Spotřeba je až o 83 % nižší než u srovna-

telných laserových tiskáren. Pokud tedy provozujete větší množství tiskáren, mohou úspory za energii představovat položku v řádu desítek tisíc korun za rok. Nižší spotřeba elektrické energie Heat-Free technologie má také enviromentální rozměr v podobě redukce množství CO2. Společnost Epson se spojila s časopisem National Geographic v kampani pro zvýšení povědomí o tom, že šetření energií a teplem je skvělý způsob, jak minimalizovat náš vliv na životní prostředí.

Významná je u inkoustových zařízení také úspora času a pokud platí, že čas jsou peníze, každý kratší pracovní proces přináší finanční úsporu. Inkoustové tiskárny jsou mistrem v rychlosti tisku krátkých dokumentů do 3-5 stran, kterých je v dnešních kancelářích většina. To tyto tiskárny odlišuje od laserových tiskáren nejen stejné, ale i vyšší rychlostní kategorie, protože inkoustová tiskárna vytiskne 3–4stránkový dokument dříve, než se laserová stihne připravit (zahřát) před tiskem. Uživatel tak neztrácí čas při čekání na výtisk. Další časovou úsporu představují vysokokapacitní zásobníky inkoustu ať ve formě zásobníků až na 84 000 stran či dolévacích zásobníků EcoTank tiskáren, které není potřeba často měnit či doplňovat. Inkoustové tiskárny mají minimum vyměnitelného spotřebního materiálu v průběhu své životnosti, neztrácíte tak čas čekáním na servis a provedení pravidelné údržby. Inkoustové tiskárny Epson lze vzdáleně monitorovat prostřednictvím cloudového řešení Epson Remote Services, pomocí kterého může zajistit váš partner plynulé dodávky inkoustů, kontrolu stavu počítadel a případný servis bez zásahu uživatele či IT oddělení.

Při zvyšující se ceně dopravy představuje úsporu také logistika spotřebního materiálu a likvidace odpadu. Inkoustové tiskárny používají až o 90 % méně spotřebního materiálu a obalů než laserové tiskárny srovnatelné kategorie. Úspora v dopravě a při likvidaci odpadu je tedy nesporná.

Je jen na uživateli zda si vybere výkonné tiskárny a multifunkční zařízení řady Epson WorkForce, anebo zařízení s inkoustovými zásobníky Epson EcoTank. Kancelářská zařízení Epson používají inkousty na bázi pigmentu, které se vyznačují výbornou barevností, ostrostí textu, světlostálostí pro archivní použití a odolností vůči vodě a zvýrazňovačům. K dispozici máme celou řadu zařízení, ze kterých si můžete vybrat na základě svých potřeb a požadavků na barvu, rychlost, softwarové vybavení, kompatibilitu se systémy řízení tisku, zásobu papíru a zpracování nestandardních materiálů.

Informace o metodice srovnání naleznete na www.epson.cz/heat-free-technology

Novicom – komplexní řešení kybernetické bezpečnosti

Aneb:

- **Jak plnit legislativní, metodické a technické požadavky v oblasti kybernetické bezpečnosti?**
- **Jaké jsou nástroje a služby k naplnění požadavků nového zákona o kybernetické bezpečnosti?**
- **Jak vyřešit problém nedostatku manažerů nebo architektů kybernetické bezpečnosti?**
- **Jak nákladově i procesně optimalizovat a efektivně nastavit životní cyklus správy agendy kybernetické bezpečnosti?**

Jindřich Šavel, CEO, Novicom, s.r.o.
Ing. Vladimír Karas, Security Consultant, Novicom, s.r.o.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ukládají povinným osobám vykonávat celou řadu činností v oblasti kybernetické bezpečnosti (dále jen „KB"). Některé z těchto činností jsou prováděny periodicky (např. audit KB nebo hodnocení rizik), jiné procesy jsou aktivovány vnějším podnětem (např. proces zvládání kybernetických bezpečnostních událostí a incidentů). Poznamenejme zde, že okruh povinných osob, na které se vztahují zákon a vyhláška o kybernetické bezpečnosti, byl významně rozšířen novelou vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

Každá povinná osoba (ať už se jedná o správce nebo provozovatele KII nebo VIS) musí zajistit výkon činnosti manažera KB, správci nebo provozovatelé KII musí navíc zajistit činnost architekta a auditora KB. Žádný právní předpis nehovoří o formě pracovně právního vztahu mezi povinnou osobou a člověkem vykonávajícím některou z výše uvedených rolí.

Osobou odpovědnou za provoz systému řízení KB je manažer kybernetické bezpečnosti, přičemž provoz systému spočívá vedle zavedení technických opatření mimo jiné ve vypracování a průběžné aktualizaci celé řady interních směrnic a záznamů (příloha č. 5 vyhlášky č. 82/2018 Sb. takovýchto dokumentů uvádí více než třicet) a dále v adekvátní reakci na podněty přicházející zvenčí. Dále je třeba vzít v úvahu, že každá organizace má svůj vlastní systém interních směrnic, předpisů a instrukcí, které se mohou zčásti týkat i odpovědností manažera KB, což dále činí jeho roli náročnější.

Proto je zde nástroj Novicom CCM (Cybersecurity Compliance Management), jehož úkolem je práci manažera KB usnadnit a zpřehlednit. Primárním cílem využití služby Novicom CCM je splnění legislativního souladu činnosti organizace v oblasti kybernetické bezpečnosti. Služba spočívá v zajištění Cloud prostředí, ve kterém je provozováno předpřipravené aplikační prostředí pro podporu činností manažera KB a týmu, který se podílí na zajištění dokumentace celého systému řízení bezpečnosti informací povinných osob, ať už jsou v pozici správce nebo provozovatele VIS nebo KII, a to v souladu s platnou legislativou v oblasti KB. Lze tedy říci, že služba Novicom CCM zajišťuje komplexní informační podporu práce manažera a současně jej vede celým procesem řízení KB.

Základní obsah a funkční rozsah Novicom CCM:

- vzorová dokumentace systému řízení kybernetické bezpečnosti;
- podpora komunikace mezi jednotlivými rolemi, podpora distribuce úkolů;
- obsahuje jednoduchý registr aktiv a rizik, registr zranitelností a dopadů a nástroj pro tvorbu plánu zvládání rizik;
- hlídání termínů pro splnění povinností;
- základní workflow řešení kybernetické bezpečnostní události/incidentu včetně formuláře pro reporting NÚKIBu a rozdělování úkolů podle nastavení incident response;

- podpora per-rollam hlasování v rámci řídícího výboru KB;
- podpora kontroly a auditu;
- vzory základních dokumentů používaných v rámci systému (mimo předpisy) – zápis z jednání, přezkum vedením, výroční zpráva, zápis z kontroly, auditní zpráva atd.;
- vzory podání NÚKIB (předvyplněné šablony – systém, kontaktní osoby apod.);
- upozorňuje na nové povinnosti a na reaktivní opatření.

Jak již bylo řečeno, zákon o KB ukládá povinným osobám ustanovit manažera KB, jehož povinnosti ve své příloze blíže specifikuje vyhláška o KB. Jestliže nejsou k dispozici zaměstnanci, kteří by byli schopni zastávat tuto roli, existuje řešení – outsourcing manažera nebo týmu KB. Outsourcing umožní vyhovět požadavkům zákona s nulovými investičními náklady, kdy si organizace pronajme pracovní čas manažera, který bude mít ke své práci k dispozici nejen software Novicom CCM, ale i další nástroje (Novicom ADDNET, BVS nebo ELISA), a to vše v ceně outsourcingu.

Rovněž si lze pronajmout celý *tým kybernetické bezpečnosti*, který může zahrnovat nejen *manažera kybernetické bezpečnosti,* ale v případě potřeby i *architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti* a eventuálně i *lektora kybernetické bezpečnosti.*

Architekt KB provede návrh implementace technických bezpečnostních opatření a zajistí bezpečnou architekturu informačních systémů, jejich vzájemné vazby a dohlédne na soulad implementace architektury informačních systémů se systémem řízení bezpečnosti informací.

Auditor KB prověří fungování systému řízení bezpečnosti informací v organizaci v definovaných intervalech a dle stanovených požadavků v souladu s platnou legislativou, případně se zásadami, standardy a směrnicemi organizace. Na základě zjištění zpracuje zprávu z auditu a navrhne zlepšení systému řízení kybernetické bezpečnosti.

Lektor KB pomůže prokazatelným způsobem naplnit požadavky vyhlášky o kybernetické bezpečnosti v oblasti lidských zdrojů zajištěním plánu pravidelného školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.

S detailní specifikací legislativních norem, rolí vyžadovaných zákonem a dalších specifik dané oblasti se můžete seznámit i na jednodenních nebo dvoudenních kurzech v rámci školení zkušených lektorů ze společnosti Novicom, kde si můžete vybrat z kurzů např.: Úvod do kybernetické bezpečnosti, Manažer kybernetické bezpečnosti, Architekt kybernetické bezpečnosti, Auditor kybernetické bezpečnosti, ISVS a Cloudové vyhlášky atd.

V současné době se v České republice připravuje nový zákon o kybernetické bezpečnosti, jehož smyslem je promítnutí směrnice EU, známé jako NIS2, do českého právního státu. V rámci služeb Novicom CONSULTING nabízíme nově zajištění studie dopadů transpozice směrnice NIS2 na subjekty v České republice, ve které Vám upřesníme, jaké povinnosti vyplývají z této nové legislativy a jak se na ně připravit.

Jindřich Šavel v Novicomu uplatňuje své 30leté zkušenosti z oblasti návrhů a dodávek infrastruktur, aplikačního software, systémů pro správu dokumentů a řízení procesů, tvorby a řízení firemní, produktové i marketingové strategie a budování prodejní sítě. Právě při realizaci dodávek pro efektivní správu a zabezpečení počítačových sítí se měl možnost detailně seznámit se způsoby zajištění kybernetické bezpečnosti a také se širokou nabídkou produktů kybernetické ochrany na trhu. V Novicomu pracuje od konce roku 2012, kde nejprve zastával pozici obchodního ředitele, a od května 2020 působí jako CEO.

Vladimír Karas se kybernetické bezpečnosti začal věnovat v polovině devadesátých let. V současné době je certifikovaný Lead Auditor ISO 27001, lektor a auditor dle zákona o kybernetické bezpečnosti, lektor ITSM dle ISO 20000-1 a ITIL4, lektor a Lead Auditor dle ISO 22301 a certifikovaný GDPR DPO lektor.

NOVICOM – CYBER SECURITY & NETWORK MANAGEMENT HAS NEVER BEEN EASIER

VITAKARTA
aneb když data s inteligencí tančí

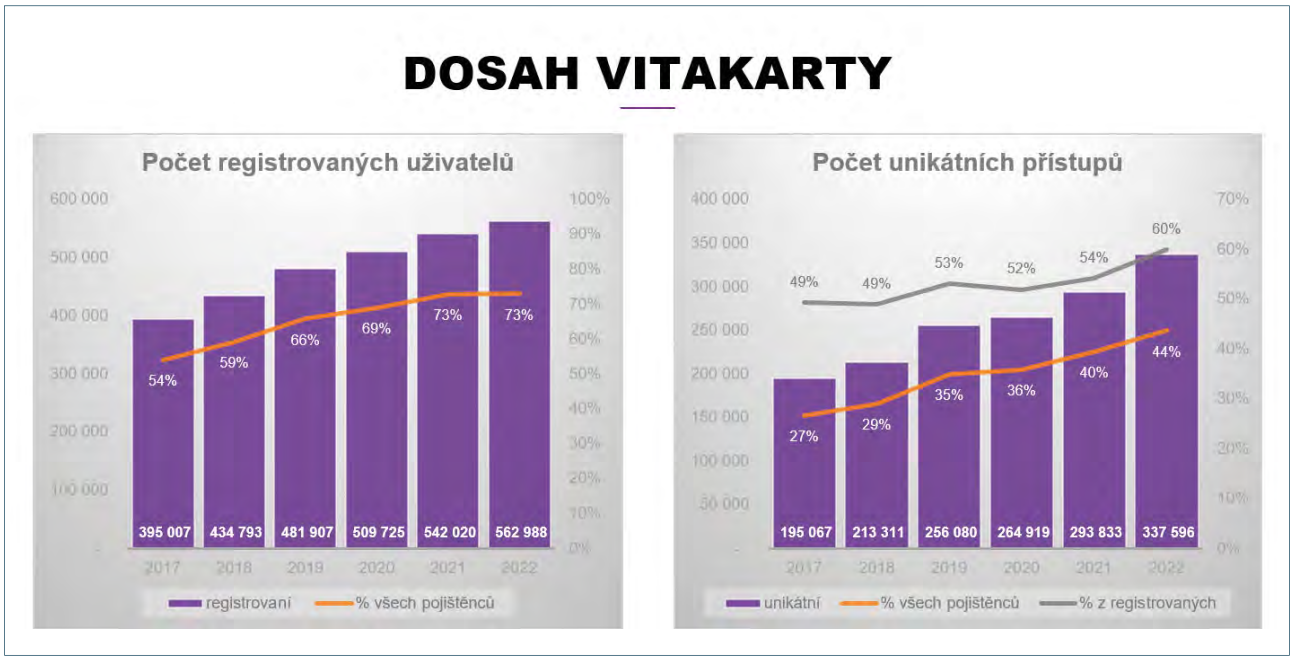
Ing. Eva Švecová, MHA – vedoucí odboru strategie, OZP

VITAKARTA je pokroková aplikace, která pro Oborovou zdravotní pojišťovnu zaměstnanců bank, pojišťoven a stavebnictví (dále jen „OZP“) představuje klíčový komunikační nástroj, jehož prostřednictvím zabezpečuje nejen své zákonné povinnosti. VITAKARTA za dobu svého dvanáctiletého vývoje drží krok s technologickými novinkami a udržuje náskok před konkurencí, což dokazuje i její vysoké hodnocení v katalogu aplikací. VITAKARTA není jen pasivní přehled vykázané péče, ale umožňuje pojištěncům jej také aktivně kontrolovat. VITAKARTA umožňuje online čerpání příspěvků z katalogu padesáti benefitů včetně využití VITASHOPU (eshopu OZP). VITAKARTA nabízí prémiové služby OZP, jako jsou online konzultace s lékaři a objednání k nim, kontrola lékových kombinací, připomínání medikace či podání přehledu OSVČ. VITAKARTA neznamená jen administrativu, ale pojištěnci jsou jejím prostřednictvím aktivně a hravě motivováni ke zdravému způsobu života a absolvování preventivních prohlídek. VITAKARTA prochází pravidelným redesignem, který modernizuje grafiku a ergonomii. Aplikace je vyvíjena a vytvářena ve spolupráci se společností **STYRAX, a.s.**

Obr. Příklady obrazovek mVITAKARTY

O užitečnosti VITAKARTY svědčí každoročně rostoucí nejen počet registrovaných klientů, ale zvláště zvyšující se počet unikátně přihlášených (v roce 2022 dokonce 337 595), viz. Obr. Čísla pro radost.

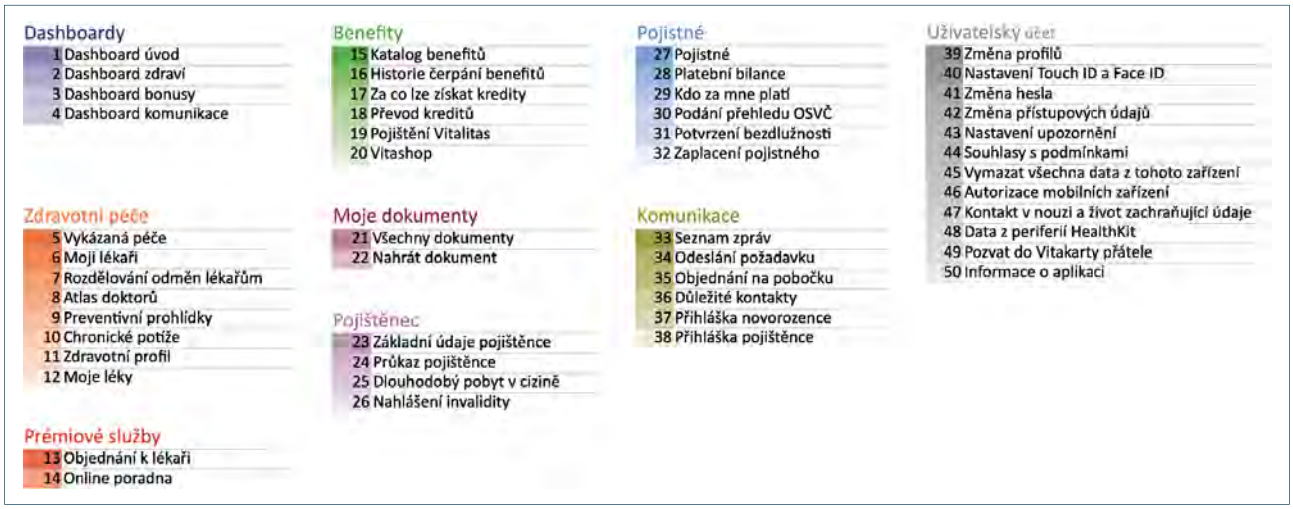
V katalogu aplikací je mVITAKARTA hodnocena 4,5 hvězdičkami pro obě dvě platformy 👍



Obr. Čísla pro radost

50 odstínů VITAKARTY

Cílem VITAKARTY bylo od počátku umožnit pojištěncům vyřídit si jakýkoliv požadavek elektronicky. VITAKARTA v současné podobě se svými více než padesáti funkcemi představuje ucelený komplexní portál online agendy OZP. Funkce z menu VITAKARTY (viz. *Obr. Menu VITAKARTY*) v zásadě obsahují všechno, co klient obvykle potřebuje řešit. VITAKARTA je tedy plnohodnotným ekvivalentem klientských kontaktních pracovišť.



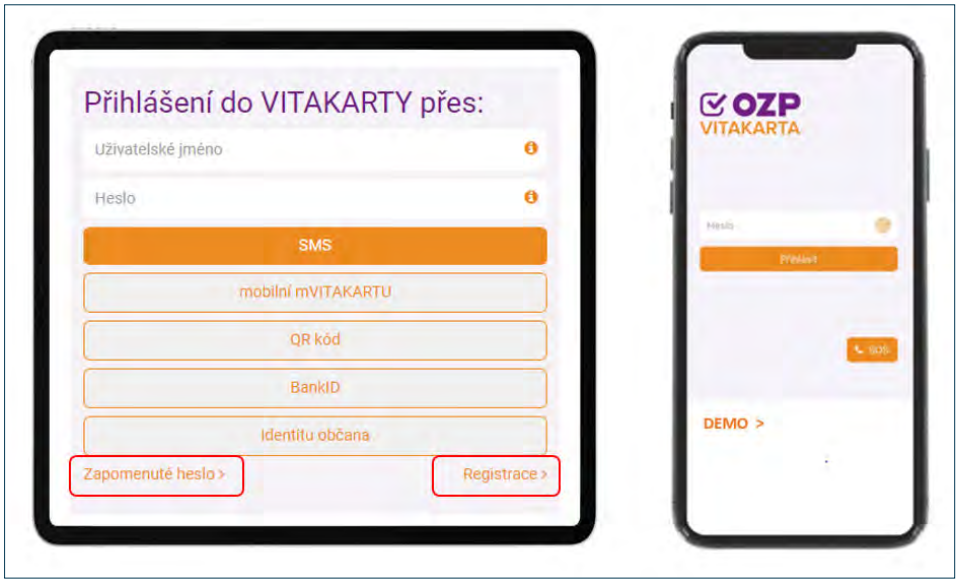
Obr. Menu VITAKARTY

Aplikace je dostupná prostřednictvím internetového prohlížeče, je k dispozici také v mobilní verzi a lze si ji stáhnout (jako aplikaci pro Android a iOS) do chytrého zařízení (mobil, tablet). Pro práci s aplikací je potřeba být klientem OZP a mít zřízený přístup do VITAKARTY. Aplikaci si ale mohou po nainstalování prohlédnout i uživatelé, kteří nejsou klienty OZP – na přihlašovací obrazovce je Demo.

Přihlášení do webové aplikace je možné prostřednictvím:

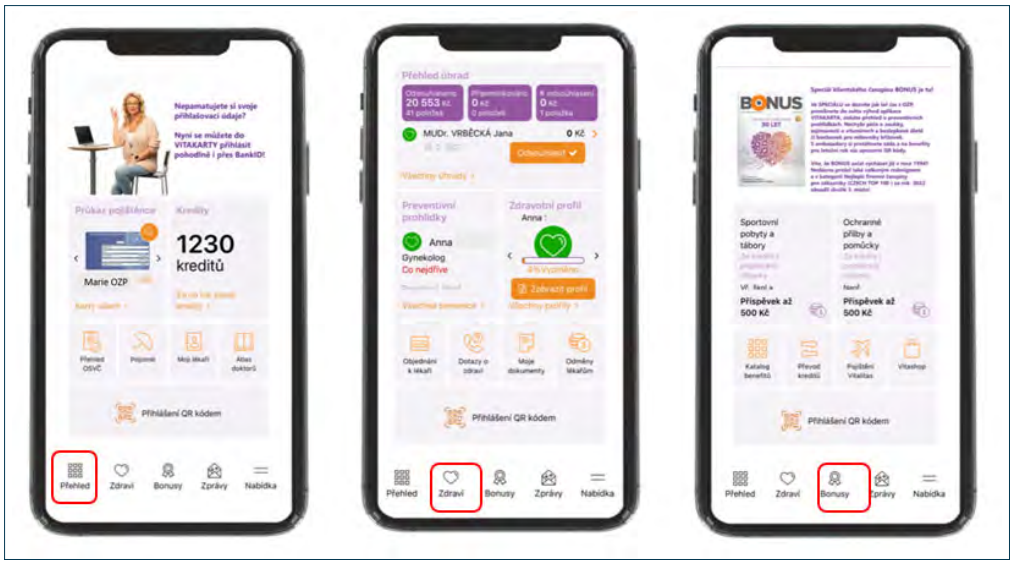
- Uživatelského jména a hesla
- Bankovní identity
- Identity občana
- Potvrzením v mobilní aplikaci
- QR kódu

Po odsouhlasení uživatelem v nastavení účtu je možné se do mobilní verze VITAKARTY přihlašovat jednoduše i pomocí biometrie (TID, FID).



Obr. Přihlašovací obrazovky

Zobrazení základních, klienty nejčastěji využívaných, služeb je na tzv. **dashboardech**, které jsou připraveny pro stěžejní oblasti ZDRAVÍ, BONUSY, ZPRÁVY a PŘEHLED. Na dashboardech jsou umístěny miniaplikace (**widgety**) zobrazující vybrané důležité informace a ikony s odkazy na konkrétní funkce VITAKARTY. Toto zobrazení vede ke snadnému ovládání a zjednodušuje přístup k hledaným informacím. Navíc odpovídá standardům, na které na které jsou klienti zvyklí i z jiných aplikací. Všechny funkcionality a služby nabízené ve VITAKARTĚ jsou k dohledání v nabídce/menu.



Obr. Dashboardy

Pojištěnci mají ve VITAKARTĚ k dispozici:

PROHLÍŽENÍ

- zdravotní vykázané péče, kterou OZP proplatila jejich lékařům (praktickému lékaři, ambulantním specialistům, nemocnicím,...),
- léků, léčivých prostředků, zdravotnických prostředků apod., na jejichž úhradě se OZP podílela,
- poplatků a doplatků, které zaplatili ve zdravotnických zařízeních a lékárnách,
- finančních refundací proplacených OZP,
- doporučené preventivní prohlídky,
- benefitů – jejich přehledu včetně možnosti okamžitého čerpání výhod,
- události řešené s Asistenční službou OZP,
- chronických potíží a rad/doporučení k potížím identifikovaným dle vykázané péče nebo označení pojištěncem v jeho zdravotním profilu.

ZAZNAMENÁVÁNÍ

- užívaných léků popř. vitamínových přípravků,
- chronických potíží,
- absolvovaných očkování,
- prodělaných úrazů, operací a zákroků,
- nemocí léčených bez návštěvy lékaře (nachlazení, virózy apod.),
- dalších údajů jako rodinná anamnéza, kousnutí klíštětem nebo pro ženy poznámky o menstruaci atd.
- hodnocení a odměn lékařů, lékáren apod.

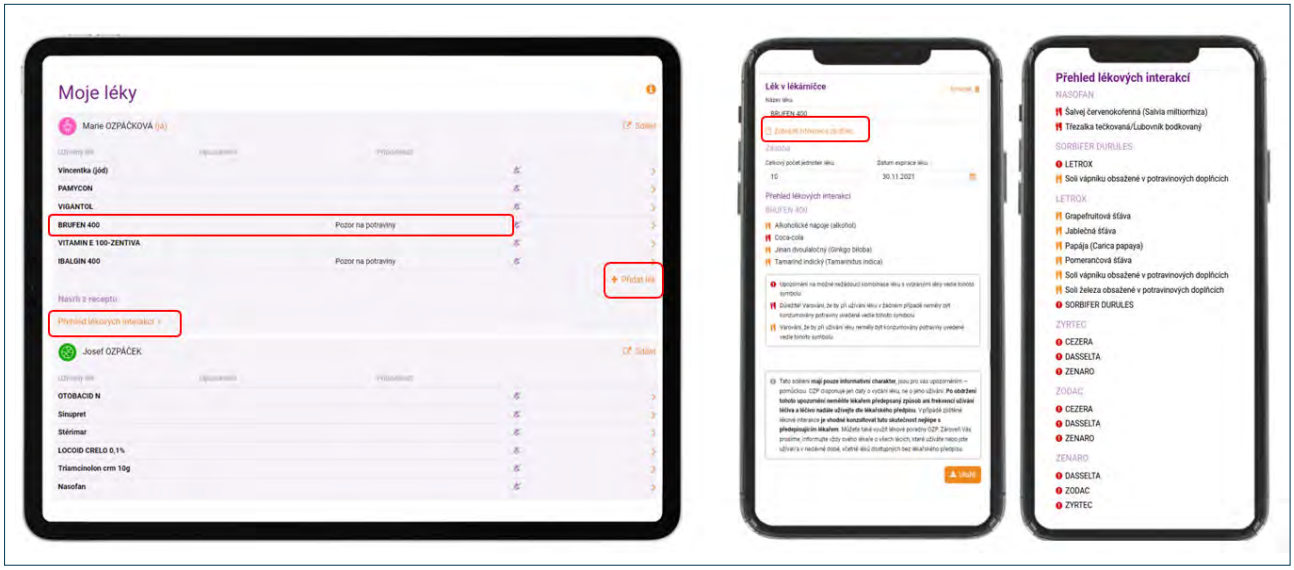
VLASTNÍ ZDRAVOTNÍ DATA

- Lze si přenášet záznamy z aplikace Zdraví (HealthKit) pro zvoleného pojištěnce prostřednictvím mVITAKARTY i do webové VITAKARTY (váhu, výšku, krevní tlak, srdeční tep a index tělesné hmotnosti).
- Tato data jsou přenášena jen na základě udělení souhlasu pro každý uvedený typ.
- Je možno ukládat soubory jako např. lékařské zprávy, výsledky vyšetření apod.

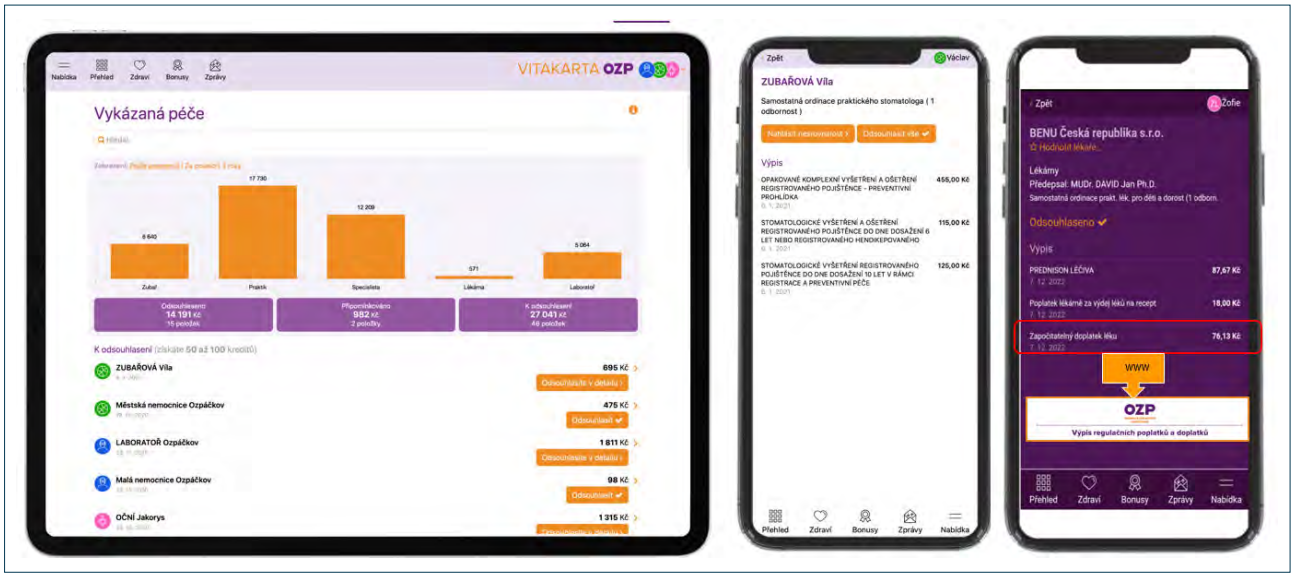
Zajímavá je i možnost využití tzv. **SOS tlačítka**, které na základě uživatelem předvyplněných údajů v případě potřeby umožňuje i bez přihlášení zavolat na předdefinované číslo, odeslat SMS nebo e-mail obsahující i údaje o aktuální poloze, popř. zobrazit emergentní údaje.

VITAKARTA
praktická aplikace pro zdraví

VITAKARTA jako významný elektronický produkt OZP představuje také názorný příklad dobré praxe využití zdravotních dat. Díky dlouholetému vývoji aplikace má OZP prostor soustředit se na tvorbu modulů, které přináší klientům značnou přidanou hodnotu. V současné podobě tak VITAKARTA obsahuje řadu pokročilých medicínských funkcí: vyhodnocuje EKG záznamy z chytrých hodinek, umí vytvořit vlastní zdravotní profil pojištěnci, hlídá prevenci ale i nevhodné lékové interakce, identifikuje chronické stavy a v neposlední řadě umožňuje jak kontrolovat vykázanou péči, tak odměňovat její kvalitu. Brzy také nabídne sdílení laboratorních výsledků. VITAKARTA jednoduše dává datům nový smysl, kdy nad nimi staví moderní inteligentní služby s informacemi pro klienta.



Obr. Přehled léků vč. detailu lékových kombinací



Obr. Kontrola výpisu péče

VITAKARTA v sobě spojuje v dnešní době nejcennější hodnoty jako je zdraví, bezpečí, čas a informace a pro uživatele je tak **praktickým a užitečným pomocníkem**.

Znalostní softwarové řešení ISIT software CZ. z pohledu směrnice NIS 2

Roman Václav, LL.M., MBA, ISIT Slovakia, s.r.o.

Úkolem nové směrnice NIS 2 je přinést vyšší úroveň kybernetické bezpečnosti v celé EU a posílit ochranu osobních údajů a kritických infrastruktur proti kybernetickým hrozbám a útokům. Směrnice NIS 2 je nástupcem a logickým pokračováním směrnice NIS odstraňující její nedostatky. Hlavním cílem směrnice NIS 2 je zvýšit úroveň kybernetické odolnosti subjektů působících v Evropské unii ve všech příslušných odvětvích a odstranění rozdílů v jejich kybernetické odolnosti v rámci vnitřního trhu. Specifickým cílem je zajistit, aby se od subjektů ve všech odvětvích, které jsou závislé na sítích a informačních systémech a které poskytují klíčové služby pro hospodářství a společnost jako celek, vyžadovalo, aby přijaly opatření v oblasti kybernetické bezpečnosti a oznamovaly incidenty s cílem zvýšit celkovou úroveň kybernetické odolnosti na celém vnitřním trhu EU.

Nová směrnice NIS 2 výrazně rozšiřuje regulovaná odvětví a již existující regulované odvětví rozšiřuje o další nové, např. poštovní a kurýrní služby, nakládání s odpady, chemický a potravinářský průmysl, výroba strojů, elektrických zařízení, automobilů a jiné.

NIS 2 zavádí taky nové požadavky pro dodavatele a poskytovatele služeb, kteří mají poskytovat služby pro kritické informační infrastruktury a digitální služby v rámci EU, a kteří musí prokázat, že zabezpečení jejich služeb a produktů bylo navrženo a implementováno v souladu s nejvyššími standardy kybernetické bezpečnosti.

Rozšířením regulovaných odvětví o nové regulované služby bude nutné, aby tato opatření přijala vhodná a přiměřená technická, provozní a organizační opatření k řízení rizik souvisejících s bezpečností sítí a informačních systémů, které tyto subjekty využívají ke své činnosti. Znamená to povinnost zabývat se základními opatřeními pro řízení kybernetických rizik ve smyslu čl. 21 Nařízení NIS 2 pro informační systémy, jejichž součástí jsou řídicí systémy průmyslové automatizace a inteligentní sítě, IoT zařízení. Z uvedeného vyplývá, že bude třeba rozšířit analýzu a řízení rizik i o průmyslové řídicí systémy – ICS (Industrial Control System) a IoT zařízení.

Nová směrnice NIS 2 předpokládá vytvoření evropské databáze zranitelností, kterou povede agentura ENISA. Do rejstříku budou zařazeny veřejně známé zranitelnosti produktů IKT nebo služeb IKT spolu s popisem dostupných opravných záplat nebo pokynů, jak lze zmírnit rizika vyplývající ze zveřejněných zranitelností. K tomuto bude potřebné řešit také otázky vhodné formy a způsobu zpřístupňování informací o zranitelnostech s predikcí zavedení využívání systémů sdílení informací s automatizovaným rozhraním pro přístup na straně příjemců těchto hlášení, s cílem cíleného upozornění na zranitelnosti rozpoznaných produktů a služeb subjektů a uživatelů.

Jedním z možných řešení automatizovaného systému cíleného upozornění na zranitelnosti rozpoznaných produktů a služeb konzumenta je implementován ve **znalostním softwarovém řešení ISIT software CZ**. Softwarové řešení ISIT software CZ v **procesně samostatném nástroji Modul Kybernetické bezpečnosti organizace** má zabudovanou funkčnost – Management **automatického příjmu a zpracování bezpečnostních varování** poskytovaných Národním centrem kybernetické bezpečnosti SK-CERT Národního bezpečnostního úřadu SK-CERT NBÚ (NUKIB) na aktuální hrozby a zranitelnosti s detekcí aktiv v informačním systému s určením ochranných opatření a upozorněním pro definované osoby v systému. Management automatického příjmu a zpracování bezpečnostních varování je ovšem jen jednou z mnoha funkcí ve znalostním softwarovém řešení ISIT software CZ a jeho Modulu Kybernetické bezpečnosti organizace.

Management automatického příjmu a zpracování bezpečnostních varování v **Modulu Kybernetické bezpečnosti organizace** je pouze doplňková funkce tohoto poměrně komplexního nástroje. Hlavním cílem, osou při vývoji tohoto nástroje byla a je snaha prakticky pomoci uživateli tohoto nástroje při správě agendy kybernetické bezpečnosti v organizaci.

Program je navržen tak, aby dokázal uživatelům i s menšími zkušenostmi v oblasti kybernetické bezpečnosti, resp. v zajišťování bezpečnosti sítí informačních systémů reálně pomoci a dosáhnut požadovaného cíle – identifikaci konkrétních bezpečnostních opatření, které je nutno implementovat na prvcích informačně-komunikačních technologiích organizace za účelem dosažení požadované úrovně odolnosti primárních procesů organizace vůči kybernetickým bezpečnostním hrozbám.

Modul Kybernetická bezpečnost organizace programu ISIT software CZ pro uživatele poskytuje v reálném čase přehled o stavu kybernetické bezpečnosti, pomáhá aktivně specifikovat zranitelná místa v zabezpečení informačně-komunikačních technologií, kybernetické hrozby, které mají potenciál tyto slabá místa využít, identifikuje a ohodnotí rizika kybernetické bezpečnosti informací. K dosažení přehledu o stavu kybernetické bezpečnosti v reálném čase pomáhá uživateli **Automatizovaná Analýza Rizik** v rozsahu automatické identifikace rizik, tzn. přiřazení relevantních hrozeb, jejich zranitelností a nápravných opatření bezprostředně po vložení, resp. zapsání aktiv uživatelem do programu, automatizované analýzy rizik, uživatelem řízený proces řešení rizik a plánu zvládání rizik.

Modul Kybernetická bezpečnost organizace programu ISIT software CZ umožňuje uživateli zabývat se základními opatřeními pro řízení kybernetických rizik ve smyslu čl. 21 Nařízení NIS 2 pro informační systémy, jejichž součástí jsou řídicí systémy průmyslové automatizace a inteligentní sítě, IoT zařízení. Modul umožňuje zařadit do procesu analýzy a řízení rizik v modulu zařadit i základní komponenty průmyslových řídicích systémů - ICS (Industrial Control System), IoT zařízení.

Kromě již uvedených funkcionalit nástroj ISIT Software CZ umožňuje:

Vedení evidence základních informací o správci nebo provozovateli základní služby, významného informačního systému, systému kritické informační infrastruktury;

Řízení personální bezpečnosti v rozsahu vedení seznamů o vlastních zaměstnancích s uvedením kromě základních personálií, procesních rolí, funkčního zařazení i informace o přístupu a přístupových oprávněních k informačním systémům provozovaných organizací, absolvovaných školeních, odpovědnostech zaměstnance, svěřených aktivech, přesunech oprávnění atd.;

Řízení třetích stran v rozsahu vedení základních informací o třetích stranách, rozsahu povolených činností, povolených přístupech, evidence smluv, seznamu a popisu třetí stranou přijímaných bezpečnostních opatření, seznamu zaměstnanců třetí strany, řízení jejich přístupů k aktivům organizace atd.;

Řízení aktiv v rozsahu evidence a popisu aktiv, evidence vlastníků aktiv, osob odpovědných za zavedení bezpečnostního opatření snižujících riziko, správce aktiv, hodnocení aktiv atd.;

Proces řízení rizik je přímo závislý na volbě souladu s požadavky na kybernetickou bezpečnost podle zvolených právních nebo obecně uznávaných norem.

Uživatelský výběr z voleb:

- volba řízení rizik kybernetické bezpečnosti podle uceleného komplexu opatření ve smyslu doporučení mezinárodně akceptovaných standardů kybernetické bezpečnosti pravidel dobré praxe (Best practices),
- volba řízení rizik v souladu s požadavky na kybernetickou bezpečnost dle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.
- volba řízení rizik v souladu s požadavky na kybernetickou bezpečnost kombinací požadavků vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. a požadavků na bezpečnost uživatelem vybraných podpůrných a technických aktiv z uceleného komplexu opatření ve smyslu doporučení mezinárodně akceptovaných standardů kybernetické bezpečnosti, pravidel dobré praxe (Best practices),
- volba řízení rizik v souladu s požadavky na kybernetickou bezpečnost podle požadavků ISO/IEC 27001: 2013/, ISO/IEC 27002: 2013 a požadavků na řízení informační bezpečnosti ve zdravotnictví ISO 27799: 2016;

Součástí Řízení rizik kybernetické bezpečnosti je vedení evidence osob odpovědných za zavedení nápravného opatření, za přijetí rizika, za přenos rizika a za společné snášení rizika;

Řízení incidentů kybernetické bezpečnosti v rozsahu evidence záznamů o incidentu, kategorii, popisu a stavu závažného incidentu, druhu incidentem zasažených údajů, zasažené moduly základní služby nebo primárního procesu, evidence důkazů, informací o kritičnosti aktiv, řešení kybernetického incidentu, zamezujících a nápravných opatření, jakož i zaslání výstupu z nástroje v předepsané formě hlášení o kybernetickém bezpečnostním incidentu na dozorový orgán, případně na jiný definovaný e-mail.

Generování závěrečné zprávy ve formě jednotlivých kapitol, resp. volitelných částí:

- Správa kybernetické bezpečnosti informačního systému
- Závěry z analýzy rizik zkoumaného informačního systému
- Aktiva
- Analýzy rizik – výstup
- Závěr
- Prohlášení o aplikovatelnosti
- Příloha 1 - legislativní východiska
- Příloha 2 – Použitá metodika
- Příloha 3 – Označení používané k zajištění sdílení citlivých informací (TLP)
- Podpůrné služby

Speciální přidanou hodnotou pro zákazníky, kteří jsou řídícím orgánem pro jiné organizace v sektorové působnosti máme připravené **multilicenční** řešení na řízení KB v rámci resortu nebo na řízení jednotlivých organizačních jednotek v robustní organizaci. ISIT software CZ podporuje a napomáhá dlouhodobě udržovat systém řízení KB v organizaci a zároveň v multiverzi umožňuje plnohodnotně řídit KB v resortních organizacích, a to včetně změn a bezpečnostních incidentů. Průvodním profitem je možnost centrální správy nastavení, seznamů hrozeb, opatření a jejich ohodnocení, ale zejména možnost centrálního systému upozorňování na HW a SW zranitelnosti, jakož i centrálního řízení zasílání hlášení o kybernetických incidentech, čímž víte jednak optimálnější analyzovat stav KB v resortu a zároveň minimalizovat možnosti vzniku bezpečnostních incidentů.

Licencování jednotlivých modulů aplikace je nezávislé, tzn. každý modul může využívat jiný počet uživatelů. Při zakoupení software v dohodnutém licencování za koncovou cenu je součástí této ceny **12 měsíců bezplatná podpora** – update. Po uplynutí 12 měsíců od instalace softwaru je možnost volitelného maintenance ve výši 15 % z pořizovací ceny na dalších 12 měsíců.

Podpůrné služby jsou Podpora při instalaci, zaškolení obsluhy pro admin a klient licence, metodická podpora při naplňování dat a realizaci tiskových výstupů, auditních činností, Analýzy rizik a Závěrečné zprávy, provedení rozdílového auditu, customizace dle požadavků zákazníka, identifikace aktiv a jiné služby v oblasti KB (samostatně placené služby).

Produkt je pojištěn na 1mil EUR - odpovědnost za způsobenou škodu pro území EU.

Modul KBO aplikace ISIT software CZ obdržel dne 12.10.2021 **Osvědčení o kompatibilitě** programového vybavení a shodě s požadavky Vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. od Fakulty podnikatelské VUT Brno.

Činnosti Úřadu pro ochranu osobních údajů z pohledu aplikace GDPR

Ing. Lenka Vaňková, Vysoká škola ekonomická v Praze,
Národohospodářská fakulta, Katedra práva

Úvod

Úřad pro ochranu osobních údajů (dále ÚOOÚ nebo Úřad) byl s účinností od 1. června 2000 zřízen zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, jako nezávislý správní orgán v oblasti ochrany osobních údajů a postupně se ujal dozoru nad dodržováním povinností stanovených tímto zákonem. Dne 24. dubna 2019 byl tento právní základ transformován na zákon č. 110/2019 Sb., o zpracování osobních údajů. Výrazné posílení ochrany dat zaznamenaly všechny státy EU od 25. května 2018, kdy vešlo v účinnost nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů neboli GDPR)[1], které představuje právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. GDPR přebírá všechny dosavadní zásady ochrany a zpracování údajů, na nichž unijní systém ochrany osobních údajů stojí a potvrzuje, že ochrana cestuje přes hranice současně s osobními údaji [2]. V souladu s tím dále obecné nařízení rozvíjí a posiluje práva lidí dotčených zpracováním, a to v obou složkách: mít informace o tom, které jejich údaje jsou zpracovány a proč; a domáhat se dodržování pravidel, včetně nápravy stavu. GDPR klade systematicky důraz na vymahatelnost práv lidí a povinností správců odpovědných za zpracování [2], podrobněji např. [3], [4], [5], [6].

Hlavními úkoly ÚOOÚ jsou monitorovat a vymáhat uplatňování obecného nařízení a dalších předpisů upravujících některé otázky ochrany osobních údajů, tedy působit jako dozorový úřad, a zvyšovat povědomí veřejnosti o ochraně osobních údajů [12].

Role ÚOOÚ při aplikaci GDPR

Úřad poskytuje zástupcům odborných, profesních a průmyslových sdružení konzultace k aplikaci GDPR. Především se vyjadřuje ke konkrétním návrhům postupů při plnění povinností uložených takovým správcům, včetně jejich vztahu s lidmi, jejichž osobní údaje tito správci zpracovávají. Konzultace poskytuje rovněž jednotlivým správcům a lidem, kteří se domnívají, že jejich osobní údaje jsou určitým správcem zpracovávány v rozporu s právními předpisy. Šířeji využitelné výstupy z konzultační činnosti zveřejňuje na svých webových stránkách a v odůvodněných případech organizuje veřejnou diskusi k návrhům metodických materiálů určených obecně správcovské veřejnosti. Zástupci Úřadu se bezúplatně zúčastňují odborných akcí s tematikou ochrany osobních údajů a Úřad se podílí i na některých vzdělávacích projektech [12].

Úřad je jediným dozorovým úřadem s obecnou působností podle GDPR v České republice; z jeho působnosti je na jedné straně vyňato zpracování osobních údajů prováděné určenými skupinami správců, na straně druhé působnost zahrnuje ochranu osobních údajů v oblastech nespadajících do působnosti GDPR. V rámci dozorové činnosti, kterou vykonává podle vnitrostátních procesních předpisů, se Úřad postupem podle správního řádu zabývá stížnostmi dotčených subjektů údajů a provádí kontrolní činnost podle kontrolního řádu a plní řadu úkolů, které sledují zkvalitnění a prohloubení ochrany osobních údajů v Evropském hospodářském prostoru i v mikrosvětě jednotlivých správců. Část z těchto úkolů se týká jednotlivých správců a zpracovatelů, např. v souvislosti s předáváním osobních údajů do třetích zemí a mezinárodním organizacím, posuzováním vlivu na ochranu osobních údajů, kodexy chování a vydáváním osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů [12].

Kontrolní činnost

Kontrolní činnost Úřadu byla v roce 2018 zásadně dotčena účinností obecného nařízení o ochraně osobních údajů. Obecné nařízení s sebou přineslo mimo jiné zásadní důraz na spolupráci dozorových úřadů jednotlivých členských států EU, která má směřovat primárně k jednotnému posuzování prováděných zpracování. Součástí tohoto systému je i mechanismus jediného kontaktního místa pro případy přeshraničního zpracování osobních údajů. Součástí kontrolního plánu pro rok 2018 byly dvě kontroly, které je Úřad povinen pravidelně provádět, tj. kontrola zpracování osobních údajů v Celním informačním systému (CIS) a kontrola zpracování osobních údajů ve vnitrostátní části Vízového informačního systému (VIS). Dále byly předmětem kontrol poznatky z předchozí dozorové činnosti Úřadu. Z tohoto důvodu proběhla například kontrola společnosti, která zpracovává osobní údaje využívané pro marketingové účely; shromažďuje osobní údaje získávané finančními poradci, kteří se společností spolupracují; dále kontrola zpracování osobních údajů u personální agentury nebo poskytovatele služeb tzv. hybridní pošty. Některé kontroly byly do kontrolního plánu zařazeny v přímé souvislosti s účinností obecného nařízení, tj. kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků. V září 2018 byl kontrolní plán doplněn převážně o kontroly zpracování systémů využívajících biometrické údaje (dynamický biometrický podpis, hlasová biometrie, technologie FaceID) [11].

V souvislosti s přijetím zákona č. 110/2019 Sb. a jeho účinností od 24. dubna 2019 došlo k reorganizaci odboru dozoru. Vznikly tak kontrolní týmy v rámci specializovaných oddělení, které doplnili dosavadní inspektory. Předmětem kontrolní činnosti v roce 2019 bylo celé spektrum povinností vyplývajících z obecného nařízení, resp. zákona č. 110/2019 Sb. Nejčastěji kontrolující konstatovali nedodržení základních zásad zpracování a absenci právního důvodu pro zpracování osobních údajů. Do kontrolního plánu Úřadu pro rok 2019 byly zařazeny např. kontroly využívání souborů cookies v soukromém sektoru, zpracování biometrických údajů, novorozenecký laboratorní screening, testování genetických údajů (DNA), kontrola politických stran v rámci voleb do Evropského parlamentu, kontrola ČSSZ zaměřená na zpracování osobních údajů prostřednictvím ePortálu, atd. [10].

Dozorové a kontrolní postupy dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád) byly v roce 2020 poznamenány situací a opatřeními souvisejícími s pandemií COVID-19. Fakticky to znamenalo utlumení určitých forem dozoru, které se zejména týkalo jak zahajování a provádění některých kontrolních úkonů, například místních šetření, tak v prodlužování lhůt pro úkony [9]. Pokles kontrolní činnosti v roce 2020 je patrný z následující tabulky, která uvádí počty zahájených a ukončených kontrol v letech 2018 až 2022 včetně uložených pokut za neposkytnutí součinnosti v kontrole.

		2 018	2 019	2 020	2 021	2 022
Kontrolní činnost (vyjma kontrol týkajících se obchodních sdělení)	zahájeno	76	63	54	52	25
	ukončeno	89	75	48	43	20
	pokuty za neposkytnutí součinnosti v kontrole	4	4	5	3	1

Tab. 1: Kontrolní činnost

Do kontrolního plánu Úřadu pro rok 2020 byly zařazeny např. kontroly zpracování osobních údajů prostřednictvím cookies provozovateli mediálně významných internetových stránek či vyhledávačů v ČR, kontroly soukromých subjektů (konkrétně poskytovatelů nebankovních úvěrů ve vztahu k pořizování a uchovávání kopií občanských průkazů), kontroly škol se zaměřením na dodržování zásad zpracování a zabezpečení osobních údajů a rolí dodavatelů informačních služeb, atd. [9].

V roce 2021 prošel Úřad zásadní změnou, která se dotkla kontrolního aparátu. K 31. květnu skončilo až na jednu výjimku funkční období inspektorů, kteří nesli primární tíhu kontrolní činnosti na základě předchozí právní úpravy, tj. zákona č. 101/2000 Sb. Tato změna přenesla těžiště činnosti na tři oddělení: oddělení kontroly veřejného sektoru, oddělení kontroly soukromého sektoru a oddělení všeobecné kontroly [8].

Úřad v roce 2022 navazoval těsnější spolupráci s úřady (např. s Českým úřadem zeměměřičským a katastrálním, Národním úřadem pro kybernetickou a informační bezpečnost, Českým telekomunikačním úřadem), které mohly s ohledem na odborné zkušenosti v oblasti své působnosti přispět k efektivnějšímu provádění kontrol v oblasti ochrany osobních údajů. Dokonce lze předpokládat, že s celkovým rozvojem digitalizace, všeobecné elektronizace komunikace a rozšiřováním využití technologií umělé inteligence bude význam takové spolupráce významně umocněn [7].

Dozorová činnost v oblasti obchodních sdělení

V důsledku nabytí účinnosti obecného nařízení o ochraně osobních údajů došlo v rámci Úřadu k jistým změnám, kdy se dozorovou činností v oblasti ochrany osobních údajů zabývají jednotlivé inspektoráty. Dozorová činnost v oblasti nevyžádaných obchodních sdělení, která byla dříve vykonávána jedním z inspektorátů, pak byla od 1. srpna 2018 svěřena samostatnému nově vzniklému oddělení, které provádí veškeré úkony spjaté s nevyžádanými obchodními sděleními, tj. především analýzy jednotlivých podání. Nejdůležitější a nejrozsáhlejší činností tohoto oddělení je provádění kontrolních a správních řízení. Neméně významné jsou však také úkony spojené s upozorněním jednotlivých subjektů na možné porušení zákona, které se provádí v případech, kdy Úřad obdrží jen několik málo stížností v určeném období vůči jednomu subjektu a zásah do soukromí v elektronické komunikaci tak není značný. Toto upozornění plní především preventivní funkci. Funkci preventivní a výchovnou či osvětovou plní také další činnosti tohoto oddělení, jako je poskytování konzultací v této oblasti a vyřizování jednotlivých písemných nebo telefonických dotazů či zobecňování výsledků kontrol a správních řízení v podobě vydávání tiskových zpráv a stanovisek [11]. Jedná se rovněž o formu spolupráce s ostatními správními úřady (především úřady na ochranu spotřebitele, Českým telekomunikačním úřadem apod.) [8]. V neposlední řadě sestavuje jednotlivé statistiky [11].

Níže uvedená tabulka zachycuje počty jednotlivých dozorových činností v oblasti obchodních sdělení v letech 2018–2022, kterými se toto oddělení zabývalo.

		2 018	2 019	2 020	2 021	2 022
Dozorová činnost v oblasti obchodních sdělení	podnětů celkem	2 901	2 007	3 031	997	906
	kontrolní řízení	30	18	16	19	-
	zahájených kontrol	22	5	15	11	12
	ukončených kontrol	17	17	8	13	10
	správní řízení za porušení zákona č. 480/2004 Sb. - řízení o sankci	26	28	20	23	30
	- celková výše sankce	3 464 360 Kč	2 099 000 Kč	7 684 000 Kč	2 901 000 Kč	828 000 Kč
	správní řízení za porušení zákona č. 250/2012 Sb. - pokuty za neposkytnutí součinnosti v kontrole	10	11	15	1	6
	- celková výše sankce	905 000 Kč	475 000 Kč	933 000 Kč	-	120 000 Kč
	vyřízeno bez zahájení kontroly upozorněním subjektu na možné porušení povinnosti	414	390	402	466	351

Tab. 2: Dozorová činnost v oblasti obchodních sdělení

V roce 2018 se oddělení věnovalo celkem 30 kontrolním řízením a s 26 subjekty vedlo správní řízení, jehož výsledkem bylo uložení sankce. Celková výše sankce, kterou toto oddělení za šíření nevyžádaných obchodních sdělení udělilo, byla 3 464 360 Kč. V deseti případech bylo vedeno rovněž správní řízení o uložení pořádkové pokuty za neposkytnutí součinnosti v rámci prováděné kontroly, kdy celková výše uložené sankce činila 905 000 Kč [11].

Převážnou část své činnosti oddělení obchodních sdělení věnovalo v roce 2019 především kontrolní činnosti a ukládání sankcí. V případech malého počtu stížností byly subjekty pouze upozorňovány na možná porušení zákona při šíření obchodních sdělení [10].

Rok 2020 byl pro oblast šíření obchodních sdělení významným, soudními rozsudky byly potvrzeny některé důležité závěry ze správních řízení, došlo též k uložení prozatím nejvyšší sankce za zasílání nevyžádaných obchodních sdělení ve výši 6 000 000 Kč, ale také došlo i k nárůstu počtu stížností na zasílání nevyžádaných obchodních sdělení zhruba o třetinu oproti předchozímu roku, což je patrné z výše uvedené tabulky. Nárůst může zřejmě souviset s pandemickou situací v roce 2020, kdy se nabídka zboží a služeb přesunula více do online prostor a tomu odpovídalo i zvýšení online propagace jednotlivých internetových obchodů, včetně šíření obchodních sdělení [9].

V roce 2021 je patrné, že došlo k významnému snížení počtu podávaných stížností. Tento pokles mohl být důsledkem dlouhodobé pandemické situace, která ovlivnila jak jednotlivé společnosti, tak i adresáty případných obchodních sdělení [8].

Oproti předchozím letům, kdy počet podaných stížností dosahoval několika tisíc, dochází i v roce 2022 v této oblasti k určitě stagnaci. Z dozorové činnosti je však patrné, že snížení počtu stížností neznamená nižší počet provedených řízení, ať už kontrolních, správních či jen formou upozornění dané společnosti [7].

Konzultační činnost a řešení stížností

Díky nárůstu počtu dotazů a posléze i k nárůstu počtu stížností subjektů údajů ve spojitosti s blížící se účinností obecného nařízení došlo počátkem roku 2018 k rozdělení oddělení stížností a konzultací na oddělení podnětů a stížností a oddělení konzultací. Stížnostní agendu výrazně ovlivnil přelom účinnosti obecného nařízení. V tomto období směřovala velká část stížností proti postupu správců osobních údajů při získávání souhlasu dotčených subjektů údajů v situaci, kdy správce neoprávněně podmiňoval poskytnutí služby souhlasem se zasíláním obchodních sdělení či jinými nikoli nezbytnými marketingovými aktivitami nebo získával souhlas manipulativně. Po účinnosti obecného nařízení zaznamenal Úřad zvýšený počet stížností na nevykonávání práv subjektu údajů ze strany správců (zejména právo na přístup k osobním údajům); na kopie veřejných rejstříků internetu, provozované soukromými subjekty; na zveřejňování osobních údajů na internetu a souvisejícího práva být zapomenut; na kamery, nejčastěji využívané v rámci sousedských (občanskoprávních) sporů, zaměstnavatelem nebo k ochraně veřejného majetku [11].

V roce 2019 převažovaly podněty a stížnosti směřující proti zpracování osobních údajů v oblasti soukromoprávních vztahů. To lze přičítat nejen vyššímu početnímu zastoupení správců v tomto sektoru, ale i povinnému jmenování pověřenců pro ochranu osobních údajů u všech OVM a veřejných subjektů, u kterých pověřenci za necelé dva roky svého působení kultivovali prováděné zpracování osobních údajů [10].

Počet podnětů a stížností v jednotlivých letech od nabytí účinnosti obecného nařízení je uveden v následující tabulce.

		2 018	2 019	2 020	2 021	2 022
Podání a stížnosti	přijaté podněty	3 616	2 482	1 855	2 430	2 192
	- vyřízeno upozorněním správce na možné porušení	462	560	452	491	785
	- předáno ke kontrole nebo jinému řízení	193	145	125	165	141
	ohlášení o porušení zabezpečení osobních údajů ve smyslu článku 33 GDPR	260	416	292	294	313
	poskytnutí součinnosti orgánům činným v trestním řízení	10	31	14	25	23

Tab. 3: Podání a stížnosti

I přes probíhající pandemii koronaviru COVID-19 došlo v roce 2020, v porovnání s předchozím rokem, pouze k mírnému poklesu počtu podnětů a stížností. Ačkoli bylo nutné vykonávat značnou část činností z domova, nebyla plynulost řešení stížností a podnětů nijak výrazněji ovlivněna. Epidemie ovšem ovlivnila obsahovou skladbu stížností a podnětů. Podatelé se na Úřad obraceli se stížnostmi a podněty, které vyvěraly z činnosti některých státních orgánů při zvládání epidemie. Z hlediska zastoupení stížností z oblastí veřejnoprávních a soukromoprávních vztahů, i v roce 2020 a 2021 pokračoval trend výrazně převažujícího zastoupení podnětů a stížností směřujících proti zpracování osobních údajů v oblasti soukromoprávních vztahů. Z nich nejčastějším zůstává zpracování osobních údajů pro marketingové účely [8],[9].

Konzultanti Úřadu především v první polovině roku 2022 v souvislosti s novelou zákona č. 127/2005 Sb., o elektronických komunikacích, vyřizovali množství dotazů v oblasti cookies. Dále úřad obdržel, obdobně jako v předchozích letech, množství dotazů ke kamerovým systémům, dlužnickým registrům, manipulacím se zdravotnickou dokumentací [7].

Účinností obecného nařízení přibylo do činností Úřadu i vyhodnocování přijatých ohlášení porušení zabezpečení osobních údajů a poskytování předchozích konzultací dle obecného nařízení. Ohlašování porušení zabezpečení osobních údajů bylo pro správce novou povinností a tak bylo možné sledovat, jak správci mnohdy nereflektovali požadavky obecného nařízení na obsah ohlášení [11]. V průběhu roku 2019 byl zpřístupněn formulář pro ohlašování porušení zabezpečení osobních údajů, který začal být záhy využíván správci z celého spektra zpracování osobních údajů [10]. Porušení zabezpečení osobních údajů, která byla ohlašována Úřadu, se vyskytovala jak v soukromém sektoru, tak veřejném sektoru [10]. Společným jmenovatelem pro oba sektory byla v roce 2018 i v roce 2019 ohlášení týkající se kybernetického incidentu, tj. napadení škodlivým programem (tzv. ransomwarem), který protiprávně zašifroval informace nebo ztráta zařízení či dokumentu [10, 11]. Roky 2020 a 2021, v nichž

Úřad obdržel stejné množství ohlášení porušení zabezpečení osobních údajů, byly ovlivněny protiepidemickými opatřeními a s tím narůstala potřeba kvalitnějšího zabezpečení internetové sítě v souvislosti se stále více rozšířenou prací z domova a s distanční výukou. Významný počet případů porušení zabezpečení osobních údajů byly nadále hackerské útoky, ať už se jednalo o phishing, ransomware, nebo jiné napadení virem [8].

Účinnost obecného nařízení výrazně ovlivnila i konzultační agendu, protože mnohdy bylo nutné mírnit paniku, která se kolem obecného nařízení vytvořila. Úřad tazatelům zdůrazňoval základní kontinuitu pravidel s dřívějším zákonem č. 101/2000 Sb.; zaktualizoval rubriku Často kladených otázek; doplňoval informační materiály na webových stránkách Úřadu; začal každodenně provozovat telefonní informační linku určenou k poskytování rychlých a jednodušších informací o obecném nařízení veřejnosti (zvláště malým a středním podnikatelům); začal provozovat telefonní linku pro dotazy týkající se kamer a kamerových systémů; odpovídal na písemné dotazy týkající se velmi různorodých otázek; objasňoval, v jakých případech vzniká, respektive nevzniká povinnost jmenovat pověřence pro ochranu osobních údajů; u dotazů na uplatňování práv subjektů údajů vysvětloval, že ani obecné nařízení nepřináší změnu tam, kde je určitý postup stanoven zvláštním zákonem; vysvětloval přísnější výklad Pracovní skupiny 29 (po účinnosti obecného nařízení nově Evropského sboru pro ochranu osobních údajů) k povinnosti vést záznamy o činnostech zpracování; poskytoval osobní konzultace; uspořádal semináře pro pověřence, atd. [11].

Ve druhém roce působnosti obecného nařízení se konzultační agenda zaměřovala jak na vysvětlování nových institutů, které toto nařízení přineslo, tak na základní principy ochrany osobních údajů platné po desítky let. Od 24. dubna 2019 byly navíc odpovědi na dotazy a konzultace poskytovány již v návaznosti i na zákony vydané k GDPR a směrnici 2016/680, které v tomto roce nabyli účinnosti – zákon č. 110/2019 Sb., o zpracování osobních údajů, a zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Vývoj počtu dotazů, které každoročně zodpovídá Úřad po nabytí účinnosti obecného nařízení, ukazuje následující tabulka.

		2 018	2 019	2 020	2 021
Dotazy a konzultace	dotazů celkem	4 161	1 836	1 571	1 651
	telefonní konzultační GDPR linka	2 800	2 667	1 351	1 091

Tab. 4: Dotazy a konzultace

Výrazné ovlivnění konzultační agendy se projevilo zvýšením celkového množství dotazů v roce 2018 a náporem na telefonní konzultační GDPR linku přetrvávajícím i v roce 2019. Telefonní informační linka k GDPR byla hojně využívána jak ze strany laické, tak odborné veřejnosti [10]. V roce 2019 počet dotazů již nebyl tak enormní, jako v roce nabytí účinnosti obecného nařízení.

Výjimečnost roku 2020 se promítla i do konzultační agendy zcela novým tématem, které ukázalo, jak úzce je ochrana osobních údajů spojena s každodenním životem. V souvislosti s pandemií koronaviru totiž vyvstaly zejména otázky, zda a do jaké míry je zaměstnavatel oprávněn zjišťovat a případně dále zpracovávat informace o aktuálním zdravotním stavu zaměstnance. Stěžejním tématem covidové problematiky však byly konzultace s Ministerstvem zdravotnictví o realizaci aplikací eRouška, užívaných k trasování nakažených osob [9].

Konzultanty Úřadu také v roce 2021 nejvíce zaměstnávaly dotazy týkající se zpracování osobních údajů v rámci opatření proti šíření pandemie COVID-19. Další podstatný podíl dotazů a žádostí o konzultace představovalo provozování kamerových systémů. K dalším tématům v rámci dotazů veřejnosti patří problematika dlužnických registrů a doby uchovávání údajů v těchto registrech. Velkou pozornost budí i téma pořizování a uchovávání kopií občanských průkazů v bankách a dalších povinných subjektech [8].

Analytická činnost

Analytické oddělení plní zadané úkoly v oblasti působnosti Úřadu již od poloviny roku 2016. Poté, co vstoupilo v účinnost v květnu 2018 obecné nařízení, význam analytické práce ještě vzrostl. Analytické zkoumání je předpokladem hlubšího chápání problémů a hledání vyváženého vztahu mezi rozvojem technologií a ochrannou osobních údajů. Analytické oddělení konkrétně

poskytuje vyjádření či rozbory k otázkám ochrany osobních údajů a soukromí státním orgánům a institucím včetně soudů, podílí se na zajišťování vzdělávací a osvětové činnosti Úřadu i na poskytování poradenství včetně spolupráce při poskytování odpovědí na dotazy veřejnosti [11]. Činnost Úřadu se odehrává na pozadí velmi dynamického vývoje evropské ochrany osobních údajů, který je v případě potřeby sjednocován v rámci Evropského sboru pro ochranu osobních údajů, a navenek může být veřejností sledován v podobě přijatých pokynů, stanovisek či doporučení k dílčím otázkám či problémům [10]. Různorodé činnosti analytického oddělení zahrnují například monitorování ochrany osobních údajů na evropské úrovni či zpracování srovnávacích analýz. Z těchto činností vystoupila do popředí již v březnu 2020 činnost spojená s ochrannou dat během pandemie [9].

Shrnutí

Ochrana osobních údajů u nás platí od roku 1992, kdy tehdy vstoupil v platnost a účinnost zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Úřad pro ochranu osobních údajů zřízený zákonem č. 101/2000 Sb., o ochraně osobních údajů, kontroloval povinnosti tímto zákonem uložené téměř dvě desetiletí, nicméně až s nabytím účinnosti obecného nařízení o ochraně osobních údajů si mnozí začali teprve uvědomovat důležitost ochrany osobních údajů [11].

Úřad pro ochranu osobních údajů je ústřední správní úřad pro oblast ochrany osobních údajů a zastává mnoho důležitých činností. Především vykonává v rámci své působnosti dozorovou, kontrolní, konzultační a analytickou činnost. Všechny tyto činnosti byly zásadně dotčeny účinností obecného nařízení.

Úřad není pouze tím, kdo kontroluje, ale také tím, kdo radí a pomáhá nastavovat prostředí v souladu s požadavky ochrany osobních údajů [10].

Kontrolní činnost byla v letech 2018–2022 vykonávaná v souladu s kontrolními plány. Dozorové a kontrolní postupy byly v tomto sledovaném období zásadně poznamenány nabytím účinnosti obecného nařízení o ochraně osobních údajů a dále pak nastalou situací a opatřeními souvisejícími s pandemií COVID-19. Rostoucí počet dotazů a posléze i stížností v souvislosti s nabytím účinnosti obecného nařízení zaznamenal Úřad i v rámci své konzultační činnosti. V roce 2020 ovšem epidemie ovlivnila obsahovou skladbu dotazů a stížností.

Oddělení obchodních sdělení, jehož nejdůležitější činností je provádění kontrolních a správních řízení, bylo rovněž ovlivněno pandemickou situací a v roce 2020 se potýkalo se zvýšeným množstvím stížností.

Literatura

[1] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Historie. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-24]. Dostupné z: https://www.uoou.cz/historie/ds-1061/archiv=0

[2] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Obecné nařízení o ochraně osobních údajů (GDPR). In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr/ds-3938/p1=3938

[3] NULÍČEK, M, a kol. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: WoltersKluwer ČR, 2017. 544s.

[4] LECHNER, T. Základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR). In: PÁNKOVÁ, K. (ed.). ISSS 2017 – Internet ve státní správě a samosprávě [CD-ROM]. Hradec Králové, 03.04.2017 – 04.04.2017. Praha: Triada, 2017, s. 45-53. ISBN 978-80-904566-9-3.

[5] VOIGT, P., VON DEM BUSSCHE, A. The EU General Data Protection Regulation (GDPR). Wien: Springer, 2017. ISBN 978-3-319-57959-7.

[6] VAŇKOVÁ, L., LECHNER, T. Dopady nového nařízení o ochraně osobních údajů na práci odhadců. Odhadce a oceňování majetku. 2018, roč. 24, č. 1-2, s. 44-57. ISSN 1213-8223.

[7] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2022. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56844

[8] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2021. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=55760

[9] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2020. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=50178

[10] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=40546

[11] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2018. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33526

[12] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Role ÚOOÚ. In: Úřad pro ochranu osobních údajů [online]. [vid. 2023-04-25]. Dostupné z: https://www.uoou.cz/role-uoou/ds-4726/p1=4726

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/38/2021.

Monet+ a ProID: Vše pro bezpečnou digitální identitu

Ivo Vrána, Product Marketing Manager, Monet+/ProID

Elektronický občanský průkaz, biometrický pas, digitální tachograf, ale i zaměstnanecké průkazy v nemocnicích a úřadech. To vše jsou produkty zlínské firmy Monet+.

Řešení pro elektronizaci dokladů

Na začátku byly běžné čipové karty, na kterých Monet+ v 90. letech vyrostl. Jejich použití se stále rozšiřovalo – nejen v bankovnictví, ale i jako nástroj pro ověření identity. Od toho byl jen krok k projektům v eGovernmentu, kde se v té době začala řešit elektronizace dokladů.

Monet+ vyvíjí vlastní software pro čipové karty i obslužné aplikace a vyrábí i vlastní hardware pro vysoce bezpečná identifikační řešení. Tato řešení musí splnit řadu bezpečnostních požadavků, zejména nařízení eIDAS, GDPR nebo Zákon o kybernetické bezpečnosti či Zákon o ochraně utajovaných informací.

Certifikační autority a výstavba PKI

Od roku 2007 dodává Monet+ PKI infrastrukturu pro elektronické doklady, tj. občanské průkaty, pasy a povolení k pobytu. Systém je od té doby nepřetržitě rozvíjen v rámci vládních institucí v ČR i SK. PKI infrastruktura odpovídá požadavkům standardu ICAO pro doklady typu ePassport, eRP, VISA Seals, nebo pro národní doklady typu eID nebo eVRC.

ProID pro digitální identitu zaměstnanců

Nástroje ProID jsou samostatnou produktovou řadou, která představuje komplexní řešení Workforce Identity – bezpečné pracovní identity zaměstnanců. Jedná se o ucelené produktové řešení, obsahující uživatelské nástroje a metody (čipové karty, bezpečnostní tokeny a mobilní aplikace) pro bezpečné dvoufaktorové přihlašování do počítačů, systémů a VPN. Toto přihlašování je například vyžadováno i novou evropskou směrnicí NIS 2.

Technologická identita

Poslední částí portfolia je řešení pro digitální identitu přístrojů, IoT a prvků infrastruktury. Jedná se o aplikaci Key Management System, která zajišťuje distribuci digitálních certifikátů a řídí jejich životní cyklus. Řešení je vhodné zejména pro Smart Metering či různé prvky OT infrastruktury.

Vše o těchto řešeních naleznete na webech www.monetplus.cz a www.proid.cz.

Úloha spisového řádu a reflexe změn předpisů

Mgr. Jiří Žouželka, Městský úřad Chrast
Mgr. Tomáš Lechner, Ph.D., TRIADA, spol. s r. o.

Role spisového řádu

Spisový řád je důležitým interním předpisem, který popisuje vnitřní fungování úřadu a stanoví základní pravidla pro konkrétní etapy životního cyklu dokumentů na úřadě od jejich přijmu až po vyřízení a uložení ve spisovně. Nedílnou součástí spisového řádu je seznam všech úřadem používaných evidencí dokumentů, upřesnění postupů podatelny a výpravny, specifikování pravidel rozdělování přijatých dokumentů a jejich následného oběhu včetně případných opravných procesů atd. Zásadní přílohou spisového řádu je spisový a skartační plán, který obsahuje seznam typů dokumentů roztříděných do věcných skupin s vyznačenými spisovými znaky, skartačními znaky a skartačními lhůtami.

Strukturu a podrobnosti zpracování spisového a skartačního plánu a také některé obsahové náležitosti spisového řádu stanoví prováděcí právní předpis k zákonu č. 499/2004 Sb., o archivnictví a spisové službě, kterým je vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby. K obsahu spisového řádu jako takového se vyjadřují i další zákony včetně správního řádu. A to znamená, že změní-li se zákon č. 499/2004 Sb., nebo zmíněná vyhláška anebo správní řád, je třeba určitě spisový řád aktualizovat. Samozřejmě to není jen o změně „textu na papíru", ale o změně fungování organizace, způsobů úřadování a výkonu spisové služby, tedy vnitřních procesů, které má spisový řád popisovat.

Protože sestavení dobrého spisového řádu, který bude správně, a hlavně maximálně věcně popisovat všechny etapy výkonu spisové služby, není jednoduchá záležitost, přišla společnost Triada již v roce 2018 s nabídkou služby celkové pomoci s přípravou této směrnice a identifikací slabých míst ve vedení spisové služby na úřadě. Za uplynulé roky již bylo sestaveno a aktualizováno velké množství spisových řádů, zejména pro menší obce, které potřebují odbornou pomoc nejvýrazněji. Nicméně tato služba byla postupně rozšiřována i pro města, kde je průběh analýzy samozřejmě obsáhlejší a každá tvorba spisového řádu vyžaduje pochopení většího množství vnitřních procesů v organizaci, a tedy i delší čas.

S ohledem na aktuální změny v oblasti legislativy týkající se spisové služby, o kterých bude řeč dále v tomto příspěvku, připravuje společnost Triada další nabídky pomoci s úpravou spisového řádu pro obce a města, a to zejména s výhledem na nadcházející dva roky, jak to odpovídá přechodnému období v aktualizované vyhlášce.

Důležité prvky procesu tvorby spisového řádu

Spisová služba je často úředníky vnímána negativním způsobem, neboť poměrně přísně formalizuje postupy a pravidla pro nakládání s dokumenty a spisy po celou dobu jejich životního cyklu na úřadu. Avšak toto precizní dodržování základních postupů úřadování a přesná evidence dokumentů je základem fungování veřejné správy již více než dvě stě let. Podle aktuálně platných předpisů je spisová služba odbornou správou dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností (blíže ke spisové službě viz [1]).

Proces tvorby spisového řádu se sestává z následujících důležitých bodů:

- Detailní mapování potřeb úřadu a stávajících pravidel oběhu a evidence dokumentů
- Sestavení návrhu nového spisového řádu podle zjištěných skutečností, a to včetně příloh
- Představení nového spisového řádu a diskuse o identifikovaných slabých stránkách výkonu spisové služby na úřadě
- Finalizace spisového řádu a jeho následná prezentace často spojená se školením

Hned první krok tvorby spisového řádu znamená, že je třeba komunikovat s jednotlivými úředníky, a to zejména těmi, kteří vykonávají specifické role při výkonu spisové služby jako je podatelna, výpravna a správce spisovny. Ale k tomu se musí přidat též nezbytné zjištění interních pravidel oběhu, zpracování, vyřizování, vyhotovování a podepisování dokumentů, a to samozřejmě na každém odboru. Již tato interakce podložená konkrétními otázkami zpracovanými do podoby dotazníku působí tak, že si jednotliví úředníci více uvědomí souvislosti a návaznosti spisové služby. Zejména pak její prolnutí s vlastním úřadováním, tedy to, že neexistuje samostatně úřadování jako výkon agend a samostatně evidence dokumentů ve spisové službě, ale že jsou to spojené nádoby, v nichž spisová služba hraje roli garanta kvality a strážce důkazních materiálů. Jasné představení účelu činností integrovaných do spisové služby pozitivně motivuje ke zvýšení kvality evidovaných informací.

Spisový řád je v rámci služby společnosti Triada sestavován jako předpis popisující skutečné fungování úřadu a upřesňující činnosti, které spadají do výkonu spisové služby. Proto je připravená nová směrnice vždy nejprve konzultována s vedením úřadu, a také s odbornými pracovníky spisové služby na úřadě. Důležitá je v této souvislosti diskuse o případných zjištěných slabých stránkách, které je vhodné upravit tak, aby se zkvalitnil výkon spisové služby a v nové směrnici tak již mohly být popsány právě tyto nové postupy.

Podceňován není ani závěrečný krok předání výsledku spojený se školením tak, aby se všichni úředníci s novou podobnou spisového řádu důkladně seznámili a aby se zároveň ještě více posílila jejich znalost v oblasti úkonů spojených s výkonem spisové služby.

Aktuální změny v oblasti legislativy týkající se spisové služby

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, byla v poslední době novelizována hned dvakrát. Obě tyto novelizace mají výrazný vliv na výkon spisové služby a dopadají právě na spisový řád.

- První ze zmíněných novelizací vyšla ve Sbírce zákonů 23. prosince 2021 a účinnosti nabyla kromě jednoho ustanovení téměř okamžitě, tedy 1. ledna 2022. To zbylé ustanovení nabylo účinnosti měsíc poté. Asi nejvýraznější změnou, byť by se to na první pohled nemuselo tak zdát, byla povinná tvorba všech dokumentů, u nichž to nevylučuje jejich povaha, v elektronické podobě pro všechny původce vykonávající spisovou službu v elektronické podobě.
- Druhou novelizací byla změna realizovaná v rámci procesu přípravy povinné atestace elektronických systémů spisové služby. Ta vyšla ve Sbírce zákonů 13. dubna tohoto roku a účinnosti nabývá 1. července 2023. Avšak obsahuje přechodné období, které říká, že veřejnoprávní původci uvedou výkon spisové služby do souladu s požadavky vyhlášky č. 259/2012 Sb., ve znění účinném ode dne nabytí účinnosti této vyhlášky, do 31. prosince 2025. Toto poměrně dlouhé období jasně ukazuje, že změn, které bude třeba zapracovat, je skutečně hodně. Jen těžko lze vybrat pouze jednu nejvýraznější, a proto zmíníme dvě. Jednak jde o povinné vkládání všech dokumentů do spisu a jednak o zrušení skartačního znaku „V“, což znamená přepracování spisových a skartačních plánů u všech původců.

Kromě toho došlo v poslední době k několika novelizacím vlastního zákona o archivnictví a spisové službě, které zasáhly např. do tvorby jmenných rejstříků a přinesly novou povinnost dodavatelům elektronických systémů spisových služeb tyto systémy atestovat a původcům používat pouze atestované systémy. I tyto povinnosti mají různě rozložené účinnosti, které všechny vyvrcholí 1. ledna 2026.

Znamená to, že bychom měli uvedenou dobu do konce roku 2025 využít k tomu, abychom zrevidovali procesy správy a evidence dokumentů a tvorby spisů v každé organizaci a následně tyto změny formalizovali do podoby upraveného spisového řádu. Z toho je patrné, že tvorba spisového řádu je vlastně takový nikdy nekončící příběh, obdobně jako třeba zajištění ochrany osobních údajů v souladu s nařízením Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, známým pod zkratkou GDPR.

Město a městský úřad Chrast

Město Chrast leží na úpatí Českomoravské vrchoviny, v nadmořské výšce 292 metrů v okrese Chrudim. Rozloha katastru je 17,8 km², spolu se svými místními částmi – Podlažicemi, Chacholicemi a Skálou, v jejímž katastru se nachází i malebné údolí Podskála. Historie města se začala psát v 2. polovině 13. století, kdy byla Chrast založena benediktinským klášterem v Podlažicích. V současné době leží město Chrast na důležitých dopravních tepnách silniční i železniční dopravy v dosahu velkých průmyslových zón Chrudim či Pardubice, zároveň však není zatíženo průmyslovou výrobou. Více informací o městě lze najít na oficiálních webových stránkách [2].

Městský úřad Chrast se skládá z finančního odboru, správního a sociálního odboru, hospodářského odboru a odboru výstavby a životního prostředí, dále z kanceláře tajemníka a úseku údržby. Do organizační struktury patří také městské muzeum. Na úřadě pracuje 19 úředníků a 20 dalších zaměstnanců. Hlavními představiteli města jsou starosta Ing. Vojtěch Krňanský a místostarostka Ing. Iva Doležalová.

Úřad provozuje elektronickou spisovou službu Munis ERMS, ve které je ročně evidováno přibližně 8000 dokumentů. Se spisovou službou pracuje přímo či nepřímo 29 uživatelů včetně starosty a místostarostky. Úřad přiděluje každému dokumentu samostatné číslo jednací v rámci základní evidenční pomůcky. Spisy jsou vedeny priorací, která je v případě elektronické spisové služby doporučeníhodným způsobem. Kontrolu vedení spisové služby stejně jako vydání spisového řádu má na starosti tajemník úřadu.

Obr. 1: Město Chrast

Spisový řád městského úřadu Chrast

Město Chrast se rozhodlo využít nabídky společnosti Triada pro tvorbu spisového řádu v březnu roku 2022. Následně proběhla návštěva konzultanta, který řízeným rozhovorem s pověřenými osobami pomohl s vyplněním obsáhlého dotazníku, jež se stal základem pro přípravu spisového řádu.

Další konzultace proběhla během tvorby spisového řádu v červnu, kdy byly upřesněny další informace týkající se změn vyplývajících z výše zmíněné novelizace prováděcí vyhlášky o podrobnostech výkonu spisové služby.

Připravený spisový řád byl úřadu představen v září 2022. V té souvislosti byla identifikována slabá místa výkonu spisové služby, avšak v případě městského úřadu Chrast jich bylo jen poskrovnu. V podstatě stačilo pouze lehce upravit podobu jednoznačného identifikátoru.

Finální podoba nového spisového řádu nabyla účinnosti dne 1. 1. 2023.

Spolupráce se společností Triada nám pomohla efektivně vyřešit problém, který se nám delší dobu nedařilo samostatně vyřešit. Vytvořit spisový řád, který bude odpovídat všem průběžně se měnícím legislativním požadavkům. Zároveň však nebude obtěžující pro práci úředníků všech odborů našeho městského úřadu, jejichž náplň činnosti je velmi různorodá. Nezávislý pohled odborníků ze společnosti Triada na celý systém spisové služby nám především pomohl tento výrazně zpřehlednit a zjednodušit. Domnívám se, že právě průběžné reagování na připomínky konzultanta přineslo málo zjištěných slabých míst na konci celého procesu tvorby nového spisového řádu. Lze však jen souhlasit s tím, že tvorba spisového řádu je vlastně nikdy nekončící proces.

Literatura

[1] KUNT, M., LECHNER, T. Spisová služba. 3. aktualizované vyd. Praha: Leges, 2022. 412 s. Praktik. ISBN 978-80-7502-616-3.

[2] Oficiální webové stránky města Chrast, dostupné na <https://www.mestochrast.cz/>.

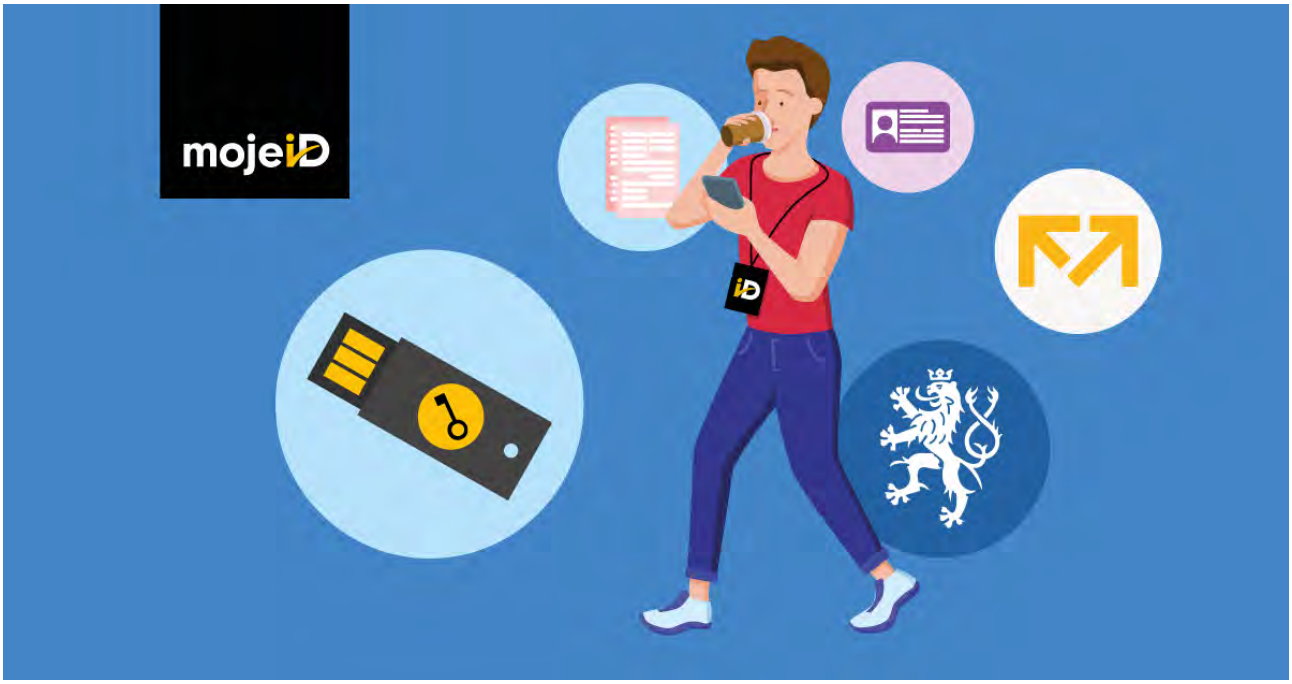
MojeID jako univerzální identifikační prostředek, nyní i za hranicemi Česka

Službu MojeID, jíž už třináctým rokem provozuje sdružení CZ.NIC, asi není potřeba zdlouhavě představovat. Jde o prostředek pro **elektronickou identifikaci**, která svým uživatelům nabízí možnost přihlašovat se k tisícům služeb v České republice s jednotnými přihlašovacími údaji – například do e-shopů či knihoven. Zároveň slouží jako bezpečný nástroj pro komunikaci s úřady a přístup k dalším online službám státní správy a samosprávy. S MojeID se ale neztratíte ani v zahraničí. Od loňského července je totiž jako **jediná česká služba svého druhu součástí evropské sítě eIDAS**. Skrz MojeID je tedy možné komunikovat i se zahraničními úřady vybraných členských zemí.

S jednou takovou možností využití MojeID nyní přišlo Německo. To nabízí **jednorázový příspěvek 200 euro pro studenty** nejen německé, ale i zahraniční, kteří v Německu studují v rámci programu Erasmus. Podání žádosti o příspěvek vyžaduje kód, který student získá od své školy, a také zřízení účtu u německé federální služby BundID. Právě k tomuto je nutné ověřit svou totožnost a tamní systém umožňuje využít digitální identity těch zemí, které jsou součástí již zmíněné sítě eIDAS.

Českých studentů v Německu asi nebudou statisíce, ale pro ty, kteří se pro vzdělání v této zemi rozhodli, je to jistě zajímavá možnost, jak získat něco navíc. Co je ale důležitější – **vzájemné uznávání elektronické identity v evropských zemích existuje a funguje**. Přistupovat k online službám v zahraničí s jednou digitální identitou je přitom možné už od roku 2018, jen musíte mít tu správnou. A tou nejuniverzálnější digitální identitou, která nabízí občanům Česka nejširší možnost využití bez bezpečnostních kompromisů, je právě MojeID.

Více informací o MojeID a jeho využití u nás i v zahraničí se dozvíte na webu MojeID na www.mojeid.cz. Detaily k německému příspěvku pak najdete na stránce www.einmalzahlung200.de.



Dopad transpozice směrnice NIS2 do právního řádu České republiky

Směrnice NIS2 a její transpozice do právního řádu České republiky, tedy návrh nového zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek, v první řadě dramaticky rozšiřuje okruh subjektů, na něž se vztahuje. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) odhaduje celkem přibližně 6 000 povinných osob.

Nový zákon o kybernetické bezpečnosti se tak dotkne subjektů poskytujících služby v řadě odvětví, z nichž nejvýznamnější jsou:

- energetika (elektřina, ropa, zemní plyn, včetně teplárenství),
- doprava (letecká, železniční, vodní, silniční),
- bankovnictví (úvěrové instituce) a infrastruktura finančních trhů,
- zdravotnictví (zdravotnická zařízení, včetně nemocnic a soukromých klinik),
- dodávky a rozvody pitné vody (dodavatelé a distributoři),
- odpadní voda (odvádění, vypouštění nebo čištění odpadních vod),
- řízení služeb informačních a komunikačních technologií,
- veřejná správa,
- poštovní a kurýrní služby,
- nakládání s odpady,
- výroba, produkce a distribuce chemických látek,
- výroba, zpracování a distribuce potravin,
- výroba zdravotnických prostředků, počítačů a optických přístrojů, elektrických zařízení, motorových vozidel, přívěsů a návěsů,
- a další.

Vedle přidání nových odvětví, na základě jejich ekonomické a společenské kritičnosti, směrnice NIS2 zároveň přidává kritérium velikosti subjektu ve smyslu doporučení Evropské komise č. 2003/361/ES, které stanovuje kritéria pro určení toho, zda je určitá společnost mikropodnik, malý nebo střední podnik. Je důležité si uvědomit, že bude povinností každého podnikatelského subjektu, aby sám posoudil, zda je či není povinnou osobou a v jaké úrovni povinností.

V první řadě je stanovena povinnost subjektů přijmout vhodná, přiměřená a odpovídající technická a organizační opatření k řízení bezpečnostních rizik a zajištění kontinuity činností.

Národní orgán dohledu již předložil návrh nového zákona o kybernetické bezpečnosti a jeho doprovodných vyhlášek, přičemž odborná veřejnost nepředpokládá v procesu schvalování zákona výrazné změny; návrh kopíruje směrnici NIS2, a tak výrazné změny v podstatě nejsou možné.

Přijetí tohoto zákona a vyhlášek se předpokládá v polovině roku 2024.

Společnost Novicom, s.r.o. je připravena pro subjekty v ČR zpracovat studii zajištění kybernetické bezpečnosti organizace. Studie stanoví dopady nové národní legislativy na organizaci a její zpracování bude probíhat v následujících krocích:

1. Posouzení, zda je organizace povinným subjektem (poskytovatelem regulovaných služeb) a stanovení úrovně povinností (nižší úroveň/vyšší úroveň).
2. Analýza současného stavu zajištění kybernetické bezpečnosti v organizaci.

3. Analýza dodavatelského řetězce.
4. Zpracování rozdílové analýzy vzhledem k úrovni povinností.
5. Definice jednotlivých projektů a odhad jejich časové a finanční náročnosti.

Náročnost zpracování studie lze (v závislosti na velikosti organizace) odhadnout na tři až šest týdnů.

Výstupem bude materiál popisující jednotlivé kroky, které je třeba učinit, aby organizace vyhověla předpokládanému znění nového zákona o kybernetické bezpečnosti.

Zajímají vás další informace k této studii? Kontaktujte společnost Novicom na e-mailu consulting@novicom.cz.

NOVICOM – CYBER SECURITY & NETWORK MANAGEMENT HAS NEVER BEEN EASIER

PREDNY SLM

software licenses management

Licence z volného trhu

Levnější cesta k pořízení totožného řešení

Úspora až 80 % oproti Microsoft CSP

Zvolte jistotu pro licencování produktů Microsoft z volného trhu

- Největší dodavatel licencí z volného trhu veřejnému sektoru v ČR
- Odborný tým právníků a licenčních specialistů
- Absolutní transparentnost – výkup i prodej licencí s kompletní dokumentací

Naše služby a řešení

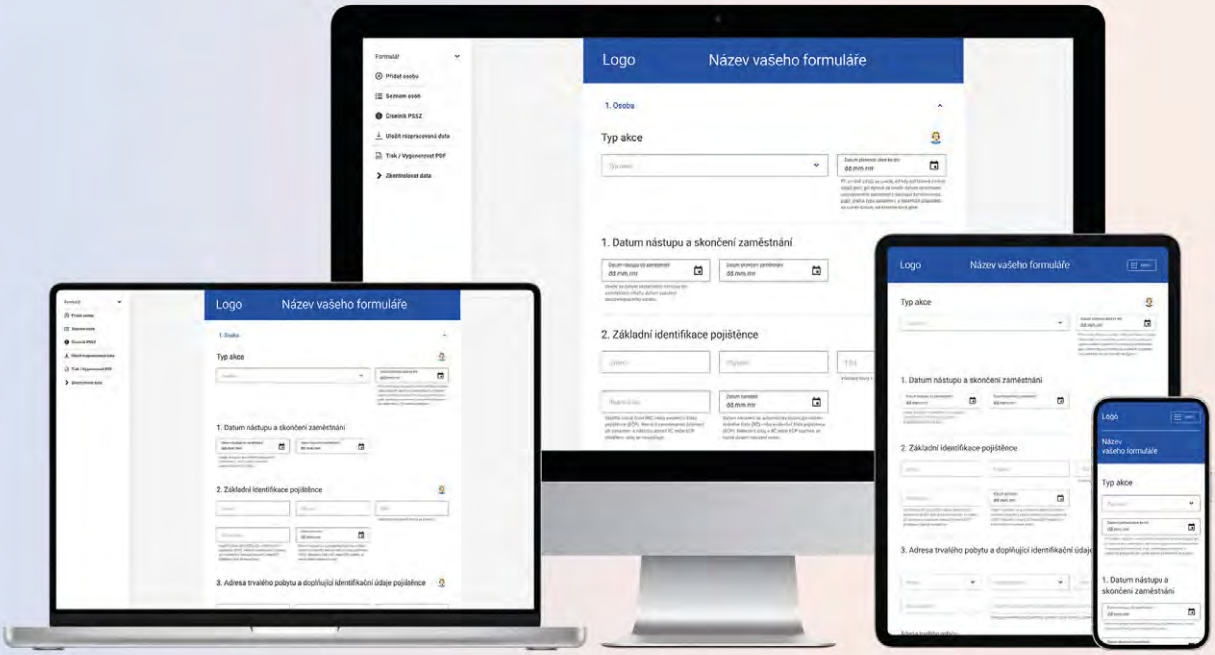
- Výkup a prodej on-premise licencí
- Optimalizace nákladů na software
- Hybridní licencování
- Licenční audity

+420 778 719 885

sales@prednyslm.eu

www.prednyslm.eu

Formuláře pro váš úřad



Formuláře od společnosti Software602 jsou připravené pro váš úřad nebo obec k rychlému nasazení. Vytvářet a editovat je můžete sami pomocí našeho webdesigneru anebo vám formuláře vytvoříme na míru.

Rychlé nasazení

Ověřené řešení

V souladu s design systémem gov.cz

Software602 a.s. | info@602.cz | +420 222 133 222 | www.602.cz

odborní partneři

Český telekomunikační úřad

MINISTERSTVO PRŮMYSLU A OBCHODU

NÚKIB

SPCSS Státní pokladna Centrum sdílených služeb

SÚKL

partneři **odborných bloků**

ATS TELCOM

STYRAX

pořadatelé

Český zavináč

ponca

TRIÁDA

Kraj Vysočina

spolupracující kraje, města, instituce

Královéhradecký kraj

HRADEC KRÁLOVÉ

Česko-Omská REGINA

ictunie

Sborník 25. konference ISSS
Editor: Kateřina Pánková
Vydavatel: TRIADA, spol. s r. o.
Rok vydání: 2023
ISBN: 978-80-907164-5-2

ISBN 978-80-907164-5-2
9 788090 716452