Egovernment
elektronizace veřejné správy

KALORIE PRO eGOVERNMENT

IROP je v rozběhu

KAPKA ZA KAPKOU

Tak se nám, jak se zdá, nastartovalo další programové období pro čerpání peněz z evropských fondů. Ono totiž s těmi ročníkovými označeními v názvu to je takové ošemetné, protože jednotlivá období mají nějaký ten určitý čas převisu, ale také takový trochu pomalý rozjezd, a tak programové období IROP 2021-2027 je administrativně umístěno počátkem do roku 2021, ale leccos se vyjasnilo až nyní. A právě o tom jsme hovořili na první letošní konferenci, kterou magazín Egovernment pořádal pod názvem FONDY, FONDY, FONDY. Některé z prezentací, které zde zazněly, jsme vzali jako základ pro toto číslo magazínu. Už proto, že z pohledu peněz, které můžeme čerpat, došlo k výraznému posunu směrem nahoru.

Není ovšem dobré jen vědět, či tušit, že mohu získat více peněz. Je rovněž dobré vědět, jaké jsou oblasti, do kterých bychom měli projekty směrovat. A nejenom kvůli fondům, ale především kvůli nám, lidem, kteří jsme klienty veřejné správy. Mělo by jít o to, vylepšit podmínky v rámci e-governmentu, tedy elektronických služeb veřejné správy. Ten náš je stále, podle různých hodnocení, spíše pod průměrem, alespoň v Evropě. Sice se každý rok vzájemně ujišťujeme, jak máme skvělý základ pro plně funkční e-government, jak jsme dobře připravili zásadní projekty a že teď už jsme nastartovali vzestupový mód, ale při závěrečném hodnocení se zřejmě pokaždé někde něco pokazí.

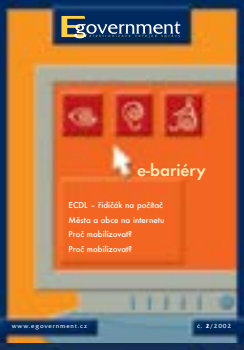
Ale nejde vlastně ani tak o konkrétní pozici v konkrétním žebříčku. Jde spíše o to, zda uživatelé skutečně užívají nabízené služby, jsou s nimi spokojeni a jejich nabídku považují za dostatečně širokou. I proto se v tomto čísle zabýváme možnostmi kudy kam tu otevřenou „pípu“ směrovat, abychom si, kapku za kapkou, vystrojili skutečně báječnou hostinu.

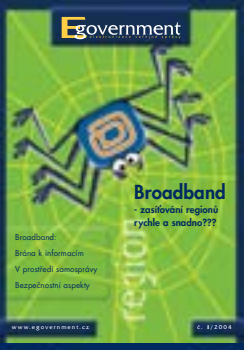
Pěkné čtení

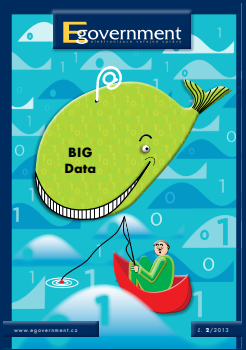
Michal Jirkovský,
šéfredaktor

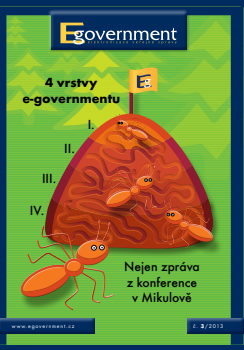
Egovernment

elektronizace veřejné správy









Vše o elektronizaci veřejné správy
- srozumitelně a zdarma:

www.egovernment.cz

Obsah

V rámci České a Slovenské republiky vydává:
info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze
pod č. C – 81357
tel.: 241 412 518
e-mail: egovernment@egovernment.cz
http: www.egovernment.cz
twitter: @EgovernmentMag
facebook: @EgovernmentMagazin

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Kateřina Alexová

Grafika: PROPAGANDA, Malá Štupartská 7, Praha 1
Tiskárna: A. R. GARAMOND s.r.o., Belnická 758, 252 42 Jesenice
Registrační číslo: MK ČR E 11364
ISSN 1801-9420

Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**. Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **300 Kč** bez DPH**/výtisk, tj. 900 Kč** bez DPH **ročně**.
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

OSOBNOST
eGOVERNMENTU 2022
GORDIC

více informací na www.egovernment.cz

Stav příprav IROP 2021–2027 v oblasti e-governmentu a kybernetické bezpečnosti

S Alešem Pekárkem jsme v úvodu jeho vystoupení na konferenci FONDY, FONDY, FONDY diskutovali o tom, zda je vlastně název jeho prezentace správný, když na začátku roku 2022 hovoří o přípravě programového období počínajícího rokem loňským. Připustil, že to zní zvláštně, ale jednotlivá programová období vlastně nezačínají úplně striktně, jak je vymezeno jejich letopočtem v názvu. Je to dáno tím, že celý záměr programového období musí být vyhlášen Evropskou komisí, přičemž Česká republika měla podklady připraveny už minulý rok. Za tuto rychlost jsme byli mimo jiné pochváleni.

Příprava tohoto programového období tedy vrcholí právě nyní. Programový dokument je oficiálně zaslán do EK. Zde se celý proces maličko pozdrží mimo jiné i tím, že EK má řadu direktorátů, které mají k dokumentu co říci a musí jej posoudit. Přitom celkově musí v současném okamžiku posuzovat 700 programů z celé EU. A samozřejmě, jako vždy, platí, že ta programová období jsou s tříletým přesahem, tedy se vlastně překrývají a vzájemně doplňují.

Aleš Pekárek pak především představil

KONKRÉTNÍ AKTIVITY V RÁMCI SPECIFICKÉHO CÍLE 1.1 EGOVERNMENT A KYBERNETICKÁ BEZPEČNOST

1. **Klasická elektronizace služeb veřejné správy** – jde o jakýkoliv e-health, e-justice, či jinou elektronickou agendu státu (typicky se může jednat například o digitalizaci stavebního řízení, což je bezpochyby služba, u které je skutečně žádoucí, aby byla digitalizována).
2. **Elektronická identita** – tady se jedná o potřebu zajistit rozvoj a aplikace elektronické identity občanů a firem pro použití v elektronických službách veřejné správy.
3. **Rozšíření propojeného datového fondu** – jedná se o pořízení prostorových dat a další rozšíření o informační systémy, které chybějí a je vhodné je doplnit. Typickým příkladem v tomto směru je digitální technická mapa.
4. **E-government cloud** – sjednocení služeb (například jednotný e-mail, jednotný web ...).
5. **Automatizace (robotizace) zpracování digitálních dat** – např. automatické snímkování aut překračujících povolenou rychlost a následně robotické vydávání a rozesílání pokut bez zásahu úředníka. Zde bude patrně způsobilý výdaj i samotné koncové zařízení, tedy radar.
6. **Portály obcí a krajů** – to je aktivita, o kterou bude patrně velký zájem. Souvisí to s navázáním na Portál občana a s celkovou propojeností služeb e-governmentu.
7. **Metropolitní, krajské a další neveřejné sítě veřejné správy** – v tomto období byl mezi podporované aktivity nově zařazen rozvoj metropolitních, krajských a dalších neveřejných sítí veřejné správy. Jde o podporu dalšího rozvoje, kdy stávající sítě potřebují něco dobudovat, modernizovat, případně upravit topologii. Aleš Pekárek upozornil na skutečnost, že s touto aktivitou se kříží strategie vysokorychlostních sítí z MPO. Právě proto tu doporučuje přečíst speciálně kapitolu, která hovoří o nárocích na neveřejné optické sítě. Zkráceně jde především o to, aby nebyl nijak ohrožen komerční trh.
8. **Kybernetická bezpečnost** – jako příklad uvedl Aleš Pekárek komplexní zabezpečení nemocnice, což rezonuje se současnou situací. Ve spolupráci s NÚKIB vytvoří MMR pravděpodobně nějaký povinný „checklist“, aby se jím žadatel zavázal k nákupu technologie, která bude následně skutečně fungovat směrem k zabezpečení dané instituce – bude to někdo obsluhovat, zároveň bude nějak ověřena instalace a provoz atp.

V této souvislosti Aleš Pekárek upozornil, že uvedené typické příklady jsou spíše jakési modelové projekty pro inspiraci. Platí ale, že jemu ani jeho oddělení nijak nepřísluší veřejné správě předkládat návrhy projektů. Naopak samotné úřady by měly cítit, jaké projekty potřebují realizovat a podpořit. Pokud je někdo, kdo může komentovat, kam se e-government v ČR má posouvat, pak je to MV ČR.

KLÍČOVÉ PARAMETRY PRO SPECIFICKÝ CÍL 1.1.

Všechny projekty budou muset získat souhlasné stanovisko hlavního architekta e-governmentu (MV ČR). Pro obecní, případně krajské projekty připravuje hlavní architekt zjednodušený formulář, ve kterém by neměly být obsaženy položky, které jsou zaměřeny spíše na velké, státní projekty.

Z pohledu Evropské komise je nutné zajistit soulad s národní strategií. V našem případě se jedná o strategii Digitální Česko. Podle Aleše Pekárka je toto klíčová podmínka pro to, aby Komise projekt schválila. MMR proto vytvořilo ve spolupráci s MV a RVIS tzv. implementační plán strategie, v němž jsou uvedené podmínky podrobně rozepsány. Plán je k dohledání na webových stránkách MV ČR.

Důležité je, že všechny projekty státních institucí musí být předem schváleny RVIS. Projekty krajů a obcí nemusí být zahrnuty v tomto implementačním plánu, ale je důležité, aby byly v souladu s výše popsanými aktivitami.

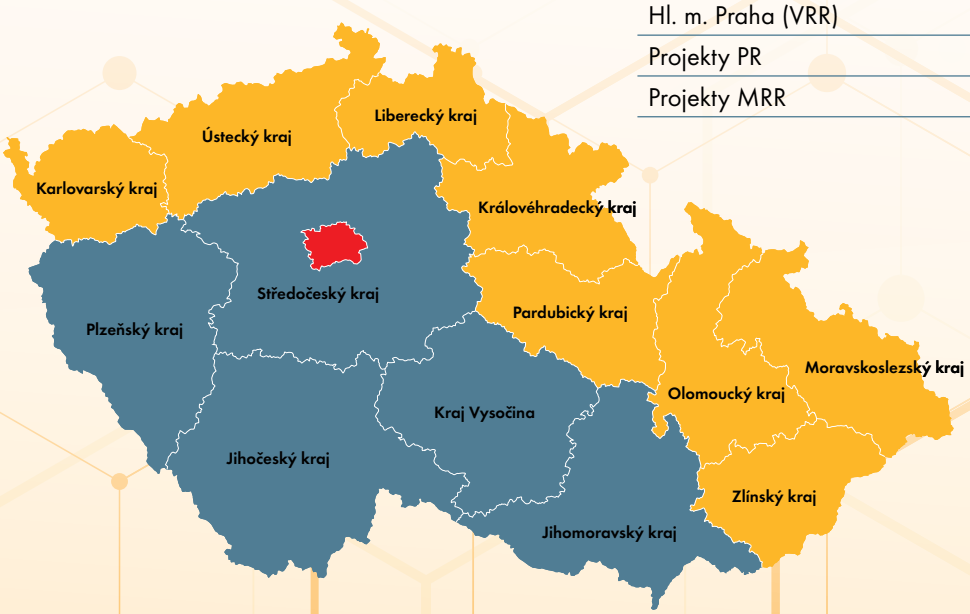
Aleš Pekárek rovněž upozornil, že určitou novinkou je v tomto programovém období možnost realizace projektů v hl. m. Praze. Praha z IROP nikdy placená v podstatě nebyla, neboť měla vlastní operační program. Ten nyní není k dispozici, a proto byla Praha „naroubována" do IROP s tím, že byla nasazena větší alokace pro více rozvinutý region. V tomto směru by měla být vyhlášena jedna výzva na všechno, v jejímž rámci může o podporu žádat magistrát, MČ i městské organizace.

MONEY, MONEY, MONEY ...

Důležité jsou peníze. Nyní je k dispozici více peněz než v předchozím programovém období (konkrétně 12,5 mld. Kč). Souvisí to s prioritami EK, kdy je věnována výrazně větší pozornost digitalizaci – mělo by se však vždy jednat o novou službu s přidanou hodnotou.

Kategorie regionů a míra spolupracování

Projekty OSS, PO OSS a další s celorepublikovým dopadem	66 %
Hl. m. Praha (VRR)	40 %
Projekty PR	70 %
Projekty MRR	85 %



Alokace jsou rozděleny na tři základní aktivity – **e-government** (6,2 mld. Kč), **e-health** (2,5 mld. Kč) a **kybernetická bezpečnost** (3,7 mld. Kč). V rámci těchto aktivit je celá ČR rozčleněna na tři kategorie regionů – **více rozvinuté regiony, přechodové regiony a méně rozvinuté regiony**.
Rozdělení uvedených prostředků v rámci aktivit je do těchto kategorií regionů směrována na základě matematických kritérií daných EK, z nichž vyplývá míra kofinancování, která činí 40 % pro hl. m. Prahu, 70 % pro přechodové regiony a 85 % proměně rozvinuté regiony a k tomu je samozřejmě možné počítat s určitou podporou ze státního rozpočtu tak, že se v podstatě celková finanční podpora pro jednotlivé typy regionů vyrovná.

Aleš Pekárek následně představil tzv. indikativní plán, podle kterého by měly být tyto programy schváleny v červnu (nejen IROP). Následně bude MMR vyhlašovat výzvy (celkový počet zhruba 200) v logickém sledu. První výzva by se měla týkat kyberbezpečnosti a mohla být vydána na konci června. Jednotlivé výzvy budou jednorázové, a jakmile se vyčerpají, už nebude další možnost. Jak bylo řečeno, první v pořadí by měla být výzva na kybernetickou bezpečnost, následně e-government a pak teprve e-health, kde budou specifická kritéria s ohledem na skutečnost, že příjemci budou zdravotnická zařízení atd.
Závěrem Aleš Pekárek uvedl, že pro MMR je hlavním indikátorem informační systém, a připomenul, co všechno musí tyto splňovat.

Projekt musí přinášet inovace v podobě nových funkcionalit informačních systémů. Každý pořízený (nový nebo inovovaný) informační systém musí mít projektem zavedeny minimálně tři nové funkcionality, například z níže uvedených:

- nová samoobslužná služba veřejné správy z Katalogu služeb veřejné správy;
- přispívání do propojeného nebo datového fondu veřejné správy;
- interoperabilita na území státu pomocí referenčního rozhraní veřejné správy s přesahem i např. v rámci EU;
- logická centralizace a celoplošná dostupnost v rámci orgánů veřejné moci (OVM) a soukromoprávních uživatelů údajů (SPUU) sdílejících informační systém veřejné správy nebo soukromoprávní systém pro využívání údajů;
- zvýšená spolehlivost, bezpečnost a průchodnost provozních informačních systémů, spravovaných jednotlivými OVM s využitím sdílení ICT platforem;
- lepší dostupnost služeb veřejné správy nebo interoperabilita na území státu s přesahem v rámci EU;
- využívání služeb Národního bodu pro identifikaci a autentizaci;
- zavedení metod automatizace a robotizace ve veřejné správě;

využívání služeb cloud computingu z Katalogu služeb cloud computingu;
budování informačního systému veřejné správy s podporou samostatných a oddělených modulů (kontejnerů) komunikujících pomocí mikroslužeb se zabráněním vendor lock-in.

Celou prezentaci, včetně videozáznamu vystoupení Aleše Pekárka naleznete na www.egovernment.cz v sekci Jihlava pod odkazem na ročník 2022.

ROK INFORMATIKY

2022

Speciální setkání úplně všech, pro které je důležitá
informatika a elektronizace veřejné správy
na úrovni krajů, měst a obcí.

Plzeň – Darovanský dvůr, 1. – 3. 6. 2022

Zhodnocení vývoje ICT na krajích, městech i obcích
a diskuze o přístupu státu k eGovernmentu.

Zapsáno do diáře !!!

Informace a registrace na:

www.egovernment.cz

Kybernetická bezpečnost v hodnocení projektů eGovernmentu

Na konferenci FONDY, FONDY, FONDY hovořil o kybernetické bezpečnosti Vladimír Sedláček, architekt OHA, MV ČR, specialista na kybernetickou bezpečnost. V úvodu svého vystoupení připomněl několik kybernetických incidentů z nedávné doby v ČR i zahraničí, na kterých demonstroval nejen finanční ztráty, ale především výrazné ohrožení důvěryhodnosti dané instituce. V případě veřejné správy je právě toto zásadní záležitost. I proto je z pohledu odboru hlavního architekta zcela podstatná Národní architektura eGovernmentu. Ta shrnuje pravidla, doporučení, vzory návrhů informačních systémů na zhruba 120 hypertextových stránkách, které jsou na adrese archi.gov.cz. Podle Vladimíra Sedláčka je žádoucí, aby se skutečně každý, kdo se nějak podílí na tvorbě, úpravě či změně , ale i na běžném provozu či údržbě informačního systému, seznámil alespoň se základními principy této strategie.

Dodržení pravidel Národního architektonického rámce z hlediska vyjádření a Národního architektonického plánu z hlediska implementace a popisu je důležité při schvalování výdajů na určené informační systémy, ať už ze zákona č. 365/2000 Sb., tak na základě usnesení vlády č. 86/2020. Platí to i v souvislosti s projekty IROP, neboť bezpečnost není jenom záležitostí ICT, ale i záležitostí architektury.

SECURE BY DESIGN

Princip Secure by Design – navrženo bezpečně pro bezpečný provoz, bezpečně dodáno, bezpečně opravováno, bezpečně ukončeno a opuštěno je v budoucnu podle slov Vladimíra Sedláčka jedním ze základních principů informační koncepce ČR. Je to otázka důvěryhodnosti a bezpečnosti, proto je bezpečnostní architektura součástí Národního architektonického rámce. OHA MV ČR se spojil s Národním úřadem kybernetické bezpečnosti a zavázal se společným memorandem na realizaci bezpečnosti. OHA má z pozice hodnotitele určité představy o architektuře, NÚKIB jako technický a správní regulátor bezpečnosti má rovněž určité představy o tom, jak má taková bezpečnost vypadat. Oboje vychází ze zákona o kybernetické bezpečnosti a příslušné vyhlášky. Konkrétně v rámci Národní strategie KB stanovují úkoly 79, 80 a 85 navrhnout a zajistit plnění takových procesů vytváření a provozování systémů eGovernmentu, které budou bezpečné, důvěryhodné, spolehlivé a u kterých bude určitá míra záruk, že evidované údaje jsou skutečně spolehlivé a že z nich mohou tedy vyplývat právně závazné skutečnosti, právní vztahy a podobně.

Smyslem uvedeného memoranda je zapojení Národního úřadu kybernetické a informační bezpečnosti do procesu posuzování žádostí, a to vlastním stanoviskem. Kromě hlavního posuzovatele a odborných posuzovatelů nebo hodnotitelů přichází tedy ještě NÚKIB jako další hodnotitel, který může vznést své připomínky.

Takže všechny ICT projekty, které budou charakteru, kdy buďto žadatel je povinnou osobou podle § 2 anebo uvedl, že bezpečnostní úroveň posuzovaného informačního systému je vysoká nebo kritická, bude věnována velká pozornost tomu, co o bezpečnostní architektuře uvádí, jak o ní uvažuje. Standardní lhůta na posouzení je 30 dnů. Pokud se během těchto 30 dnů identifikuje určitý problém, lhůta se zastavuje do vyřešení. Vladimír Sedláček potvrdil, že většinou do dvou dní poté, co je projekt zaslán do spisové služby OHA, je mu přidělen tým hodnotitelů a obvykle do týdne je probírán na poradě hodnotitelů. Takže 30 dnů pro jednoduché projekty, celkem 60 dnů pro složité případy by mělo být maximum.

Formuláře (na adrese https://archi.gov.cz/uvodschvalovani#jake) jsou od začátku tohoto roku tedy rozšířeny o nové otázky, a to na bezpečnost, nakládání s osobními údaji a jejich zpracování, narušení bezpečnosti informací v informačním systému. NÚKIB v této souvislosti vydal brožuru, ve které prezentuje minimální bezpečnostní standard. Obsahuje 17 kapitol, které z části míří na manažery organizace, tedy na vedení, a z části na techniky, IT pracovníky. Nepočítá se s tím, že by celý formulář vyplňovala jen jedna osoba s jednou specializací. Tak jako v OHA posuzuje projekt tým odborníků, tak je stejně dobré, aby u důležitých projektů vystupoval tým odborníků, kteří celý informační systém připravují na všech úrovních jeho architektury a používání.

BEZPEČNOSTNÍ ARCHITEKTURA

Bezpečnostní architektura sama je takovou zajímavou disciplínou, protože prorůstá napříč všemi doménami. Patří k ní GDPR, budou k ní patřit připravované předpisy EU, jako třeba Data governance act a podobně. U nás je popis bezpečnostní architektury součástí Národního architektonického rámce (https://archi.gov.cz/nar_dokument:ramec_obsahu_a_vystupu_architektur#metamodel_bezpecnostni architektury_sa). Jak bylo řečeno, bezpečnostní architektura sama prorůstá všemi doménami, napříč není nic, co by se hodilo jen na IT pracovníky nebo „bezpečáky" či pouze na dodavatele cloudu, vedení úřadu, nebo na pracovníky na přepážkách. Každý z nich je důležitou součástí celku, celé bezpečnosti, a tudíž musí být zahrnut nebo by měl by být zahrnut do bezpečnostní architektury. Tento model primárně je tvořen (a zejména při pohledu z výšky) motivační architekturou a byznys architekturou.

Celou prezentaci a videozáznam vystoupení naleznete na www.egovernment.cz v sekci Jihlava pod odkazem 2022.

Aktuality v oblasti regulace kybernetické bezpečnosti

S tématem regulace kybernetické bezpečnosti na konferenci FONDY, FONDY, FONDY vystoupila za Národní úřad kybernetické a informační bezpečnosti Daniela Procházková. Celé vystoupení bylo rozčleněno do čtyř kapitol, které by měly být z pohledu veřejné správy v současné době aktuální.

ÚKOLY Z AKČNÍHO PLÁNU K NÁRODNÍ STRATEGII KYBEZ

Patrně nejdůležitější pasáž, tedy zabezpečení systémů e-governmentu, probral v rámci svého vystoupení pan Sedláček, a tak Daniela Procházková připomněla v dalších bodech, že proběhla analýza právních možností operativního nákupu ICT prostředků v rámci krizových stavů i v návaznosti na probíhající pandemii a další souvislosti. Na základě konzultací MMR, MV a NÚKIB bylo konstatováno, že legislativa v současném stavu je dostačující, a proto nelze očekávat další legislativní vývoj nebo změny. Pozornost věnovala rovněž vzniku podpůrného materiálu, který sloužil k zabezpečení distančního vzdělávání a byl zpracován ve spolupráci s Ministerstvím školství mládeže a tělovýchovy. Tento materiál byl již distribuován základním a středním školám.

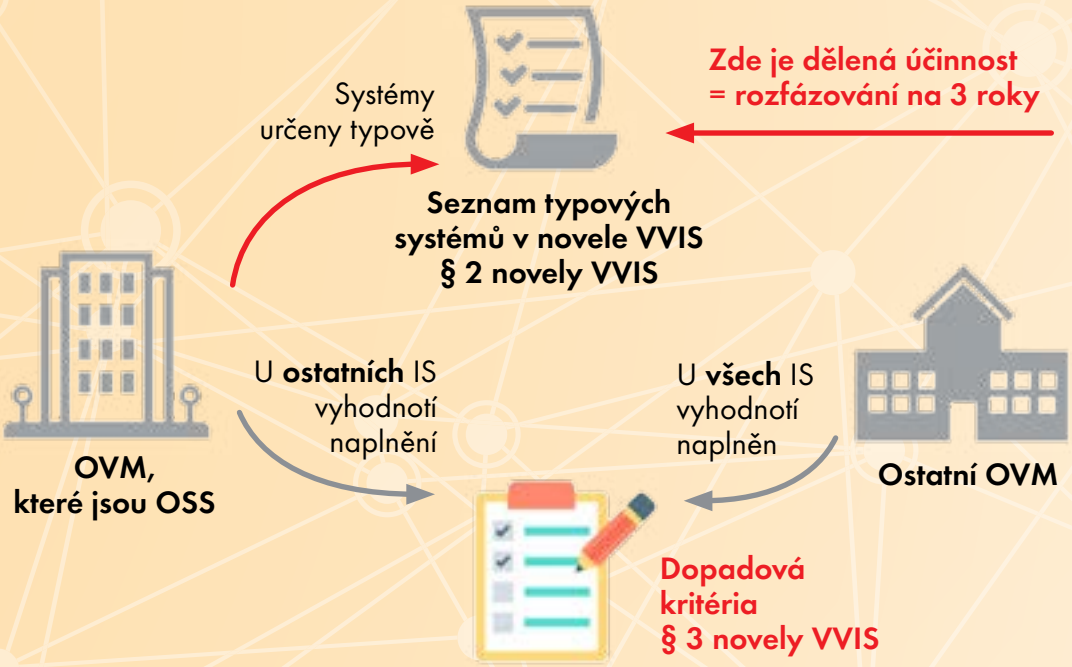
Podstatným momentem je skutečnost, že finišuje dokument, který je z pohledu povinných osob velice důležitý, a to Metodický dokument k analýzám rizik. V jeho rámci by mělo dojít ke srovnání jednotlivých analýz rizik, které se používají v rámci implementace zákona o kybernetické bezpečnosti, případně prováděcí vyhlášky. Toto srovnání, které bude k dispozici jak povinným osobám, tak široké veřejnosti, bude uzavřeno v průběhu druhého čtvrtletí.

Další povinností, která vyplývá z Akčního plánu je navrhnout jednotný postup hlášení kybernetických bezpečnostních incidentů relevantním orgánům. V současném stavu je systém těchto hlášení roztříštěný a nejednotný. Jde tedy o snahu zjednodušit tento proces. Tento úkol by měl být splněn do konce roku. Navazovat bude snaha o tvorbu jednotného rozhraní, ve kterém by se incidenty daly zaznamenávat a rozeslat hlášení většímu počtu subjektů státní správy.

Dalším úkolem, o kterém Daniela Procházková hovořila, je metodický dokument k řízení bezpečnosti dodavatelů. Jedná se o velké téma v EU, a tedy i v rámci ČR. Hotov by měl být na konci roku 2022 a opět bude k dispozici na webu NÚKIB. Poněkud vzdálenější budoucností je pak, podle Daniely Procházkové, návrh aktualizace standardů šifrování v návaznosti na kvantové počítače, stejně jako definování nějakých dalších systémů, které jsou důležité pro chod státu a nejsou zahrnuty v současné regulaci. A zřejmě v úplně nejvzdálenější budoucnosti se nachází možný výsledek snahy zpracovat návrh legislativy, která by upravovala odbornou způsobilost osob vykonávajících některou z rolí dle vyhlášky o kybernetické bezpečnosti.

DALŠÍ VLNA ÚČINNOSTI VYHLÁŠKY O VIS

Jedná se o vyhlášku, která je účinná již od minulého roku, ale vzhledem k nákladnosti byl paragraf 2 rozdělen a vznikla u něj dělená účinnost. Jen v krátkosti Daniela Procházková vysvětlila, jak vyhláška funguje.Zásadní jsou paragrafy 2 a 3. Paragraf 2 je určen organizačním složkám státu a krajům a jsou tam vyjmenovány v podstatě povinné typové systémy, které po jednotlivých letech zařazují regulaci, danou zákonem o kybernetické bezpečnosti. Paragraf 3 se týká všech ostatních netypových systémů, a tedy všech orgánů veřejné moci, které nejsou organizační složkou státu nebo krajem, a zde se posuzují dopadová kritéria.



V loňském roce se v organizačních složkách státu povinně zařazovala elektronická pošta nebo systémy sloužící ke kontrolní a inspekční činnosti. V letošním roce se jedná o větší vlnu zahrnující tři typové informační systémy. Konkrétně se jedná o systémy pro přípravu na krizové situace, dále spisové služby a vedení elektronické úřední desky. Tato vlna vešla v účinnost 1. 1. 2022. Od tohoto data běžel měsíc pro nahlášení kontaktních údajů v případě, že organizační složka státu takový systém používá pro výkon působnosti orgánů veřejné moci. Daniela Procházková připomněla, že vyhláška zavedla nebo zdůraznila určitou povinnost evidence významných informačních systémů. OVM by tedy měly evidovat, jaké systémy mají, sepsat posouzení toho, zda je zařadily mezi významné informační systémy nebo ne. Na webu NÚKIB je k dispozici podpůrný materiál, který popisuje nutné detaily k identifikaci významných informačních systémů i s příkladovou tabulkou.

NOVELIZACE SMĚRNICE NIS A DOPAD NA VS

Původně tato novela nebyla pro veřejnou správu až tak zajímavá, protože na ni nějakým způsobem nedopadala a pouze ji zaváděla do našeho právního řádu provozovatele základních služeb, kteří se vyskytovali v oblastech průmyslu. V případě směrnice NIS2 však návrh komise rozhodl zajistit, aby zahrnovala i veřejnou správu. To, jak to na konci dopadne, ještě v tuto chvíli není zcela jasné. Momentálně probíhají trialogy, jedná komise, rada i Evropský parlament ve velmi živelné podobě. Komise má skutečně velký zájem na tom, aby se směrnice novelizovala a aby se to stalo rychle. Jedná se o poměrně velkou novelu, která může být zajímavou ukázkou, jakým způsobem si EU představuje řešení kyberbezpečnosti. Dá se říci, že z pohledu EU se jedná o výrazné rozšíření toho, co by mělo být v oblasti kybernetické bezpečnosti regulováno, a to jak personálně, tak ve smyslu nových odvětví. Jedním z nich je tedy i veřejná správa, přičemž definice toho, kdo pod regulaci ze strany státu spadá a kdo ne, je dosti rozvolněná. S tím se bude muset vypořádat NÚKIB.

Vzhledem k tomu, že se toto týká tisíce právnických osob v ČR, bude patrně vhodné, aby byla definována škála toho, kdo plní jaké významné povinnosti, jaké jsou s tím spojeny nároky atp. NUKIB si již řadu osvojil relativně dost pravomocí ještě před účinností této směrnice, takže tam se toho patrně mnoho nezmění. Větší pravomoci jsou pro CSIRT týmy. Státní, nebo vládní CSIRT tým je již pod NÚKIB, a má tedy konkrétní pravomoci dány zákonem, zároveň jsou stanovena bezpečnostní opatření.

Novinky:

- hlášení relevantních událostí a hrozeb, sdílení informací o zranitelnosti (registr ENISA);
- o povinné vzdělávání managementu, větší odpovědnost (a dočasný zákaz výkonu funkce, netýká se veřejné správy);
- vyšší pokuty za porušení povinností (inspirace GDPR, nicméně zde stanoven strop; až 2 % z obratu 4 mil. EUR);
- spolupráce členských států na kontrolách a na výměně informací;
- sdílení informací mezi povinnými subjekty (stát má zajistit platformu);
- užší spolupráce NÚKIB s dozorovými orgány z jiných oblastí (ÚOOÚ, ČTÚ ...);
- do budoucna možnost povinných certifikací produktů;
- cloud computing = standardní povinná osoba;
- rozšíření působnosti NIS2, zahrnutí veřejné správy;
- způsob identifikace povinné osoby;
- rozsah regulovaných systémů.

Podle slov Daniely Procházkové se vedla obsáhlá diskuze o tom, jestli si EU vůbec může dovolit takto regulovat veřejnou správu. Některé státy, včetně ČR, vnímaly rozpor v otázce vnitřního trhu a vnitřní bezpečnosti a především braly veřejnou správu jako otázku národní bezpečnosti, do které nemá EU právo zasahovat. Na konci to dopadlo tak, že je to zahrnutelné pod vnitřní trh a tím k nějaké regulaci veřejné správy určitě dojde. Ten vývoj byl poměrně překotný a zajímavý byl první návrh toho, jak by měla vypadat regulace – zahrnovala by nějaké centrální orgány, zejména orgány NUTS1 a NUTS2. Po připomínkách by EU tento přístup korigovala stejně jako podmínku právní osobnosti. Došlo tedy následně k redefinici, která je momentálně předmětem jednání, ale odhadnout jejich výsledek je v tuto chvíli nemožné.

Z pohledu povinných subjektů by zřejmě mělo dojít k tomu, že určené subjekty zůstanou určeny, z působnosti směrnice NIS byly vytrženy pouze banky. Působnost v oblasti kybernetické bezpečnosti se v tomto směru tedy přenáší na Českou národní banku.

Jako primární kritérium posuzování bude velikost organizace, to bude kvantitativní kritérium.

Rozsah zabezpečení informačních systémů bude rozšířen na celou organizaci, tedy nejenom na systémy používané pro výkon základní služby, jak tomu bylo doposud. To je velká změna oproti dosavadní koncepci. Dojde rovněž k většímu zapojení Evropské komise, která si nově osobuje právo vydávat prováděcí akty komise. Rovněž jsou zaváděny vyšší pokuty a kladen větší důraz na sdílení informací mezi subjekty navzájem.

REGULACE CLOUD COMPUTINGU

Daniela Procházková dále prezentovala důvody pro regulaci cloud computingu ve veřejné správě.Využití cloudových služeb jak v soukromém, tak veřejném sektoru rychle roste.

Cloudové služby mohou přispět k:

- ekonomičtějšímu provozu;
- bezpečnějšímu provozu informačních systémů (centrální řízení, dohled a aktualizace).

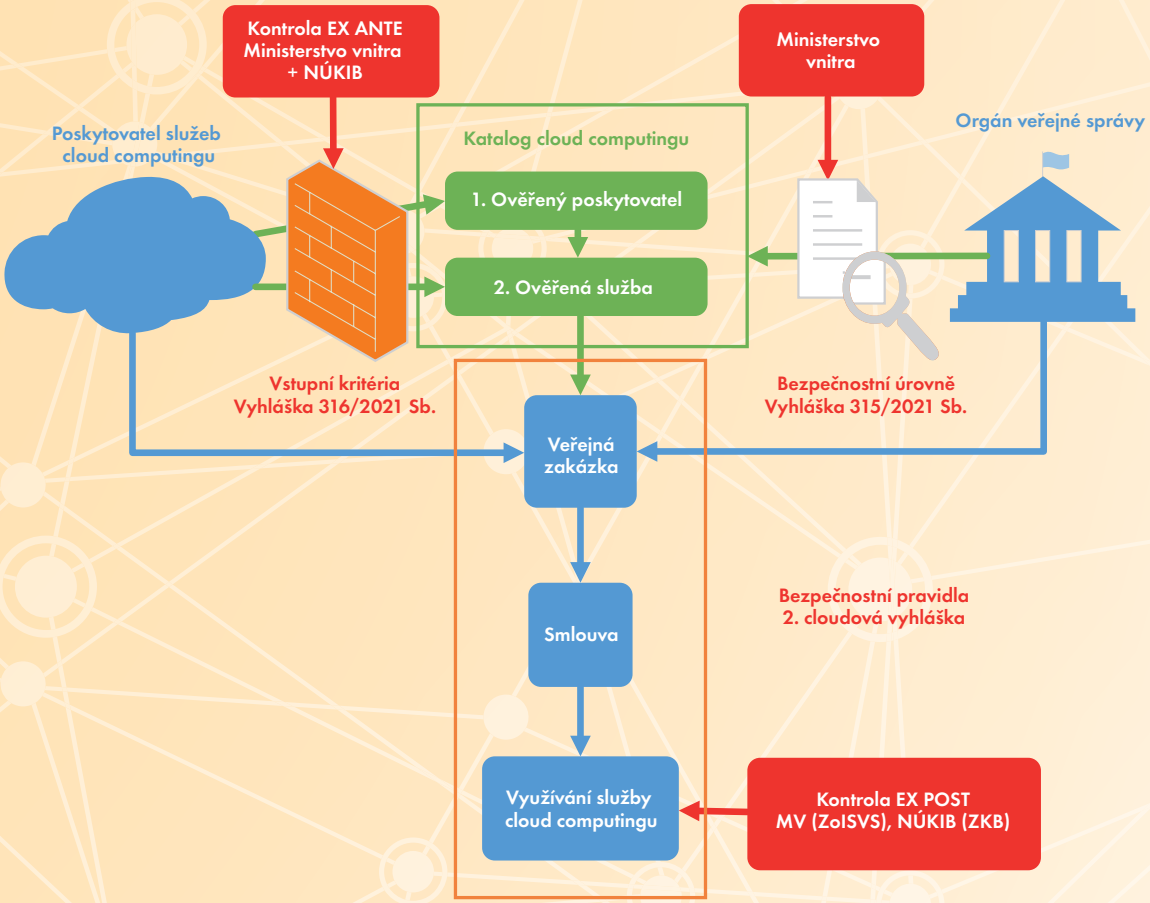
Cloudové služby však přináší i nová rizika:

- místo zpracování dat je mnohdy v zahraničí a často neznámé jednotlivým zákazníkům využívajícím cloudové služby;
- nutnost brát v úvahu i relevantní prvky právního řádu třetí země – přístup cizozemských orgánů k datům (GDPR, SD EU Schrems II);
- velká závislost na poskytovateli a omezené možnosti prověření poskytovatele.

Jak zdůraznila, regulace cloud computingu ve veřejné správě je nyní zcela na místě. Současný rozmach CC, který může být ekonomičtější pro provoz anebo i potažmo bezpečnější pro provoz, vede také k tomu, že vznikají nová rizika. Patrně tím nejzásadnějším a také třecí plochou při vyjednávání regulace je předávání dat do zahraničí a jejich zpracování v zahraničí.

V současné době jsou vydané dvě ze tří potřebných vyhlášek pro provádění těchto zákonů, a to vyhláška o požadavcích pro zápis do katalogů nebo takzvaně vyhláška o vstupních kritériích a vyhláška o bezpečnostních úrovních. Třetí se připravuje. Co se týče personální působnosti té úpravy platí, že orgány veřejné správy, které mají informační systémy VS, jsou součástí procesu zápisu do katalogu. Musí tedy nakupovat v rámci toho, co je zapsáno v katalogu.

Oblíbené schéma, které ukazuje, jakým způsobem funguje zápis do katalogu v rámci ISVS, kdy dochází k předběžné kontrole jak poskytovatele cloudu, tak poskytované nebo nabízené cloudové služby (v rámci posuzování má hlavní slovo MV ČR, NÚKIB dává stanovisko z hlediska kybez). Následně dojde k zápisu do katalogu, odkud by si ideálně měl vybírat OVM potom, co si nějakým způsobem vyhodnotí, jakou bezpečnostní úroveň má systém, který chce do cloudu umístit. Toto by se mělo spárovat a dále by mělo dojít k vzniku smluvního vztahu, ve kterém by potom měla figurovat bezpečnostní pravidla.



V závěru vystoupení Daniela Procházková prezentovala potřebné odkazy:

Vyhlášky, včetně odůvodnění: § https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/;

Nejčastější dotazy: § https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/;

Katalog cloud computingu – zapsané nabídky a poptávky: § https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3d%3d;

Služby, které trvale ukládají data mimo EU – Úřední deska NÚKIB: https://www.nukib.cz/cs/uredni-deska/ – od nové právní úpravy – zatím prázdné;

Podpůrné materiály – Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně a Požadavky na zprávy z penetračních testů v souvislosti se zápisem cloud computingu do katalagu cloud computingu: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/.

Celé vystoupení a PDF prezentace najdete na stránkách www.egovernment.cz v sekci Jihlava s letopočtem 2022.

Digitální, elektronický a elektronizující úřad

Elektronizující záležitosti

Přebujelý slovník pestrobarevných letáků, které jsou plné novotvarů a nezvyklých sousloví, je často známkou toho, že se IT firmy snaží o komercializaci nějaké agendy. Taková snaha pak produkuje všelijaká moudra. Základem je vybudovat na heslech produkt, který se prodá sám. Stačí do nabídky napsat komplexní digitální e-government a dát cenu hodně nízko. Výsledek? **Mnoho obcí si pořídilo portál občana svého města, který za poslední rok navštívilo 20 lidí**, a proběhly v něm 4 platby. Digitálně. Elektronicky. **Elektronizující záležitost**.

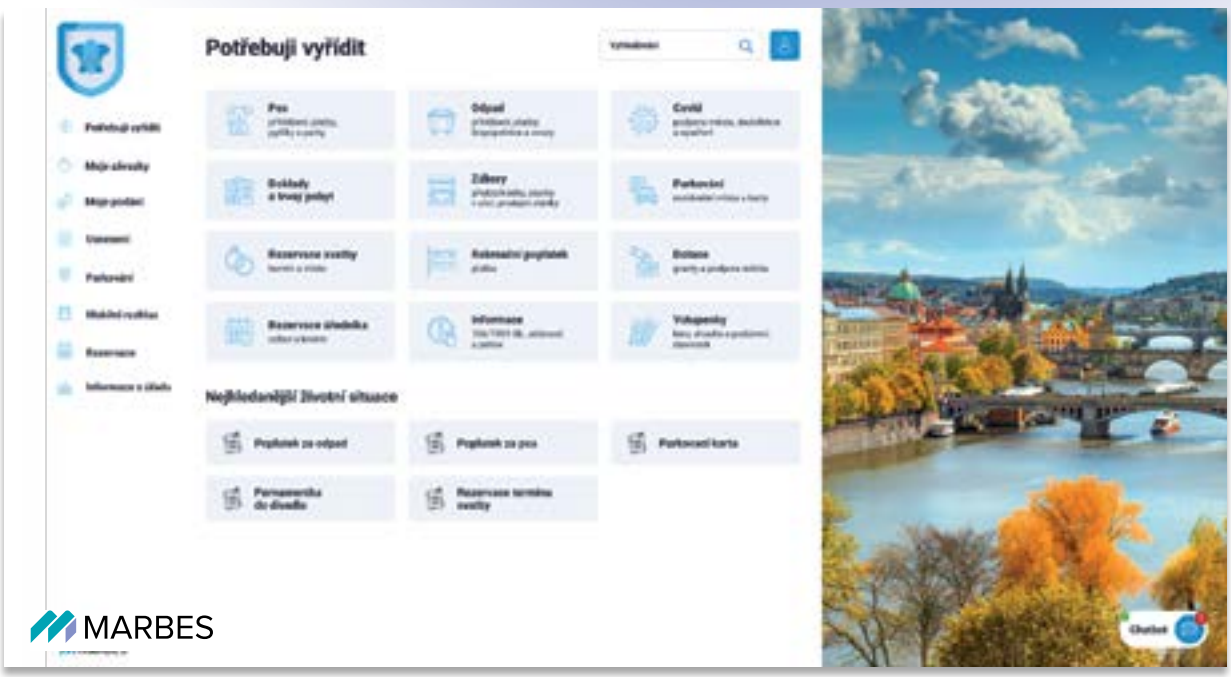
Prozradím ještě, že ty 4 platby byly testovací. **Psal jsem si pár dnů s jedním starostou, který tvrdil, že má portál občana, který je skvělý. Po otázce, jak jsou s tím řešením spokojeni zákazníci, se odmlčel.** Pozoruji poslední týdny ještě jednu podivuhodnou věc. Mnoho výborných „ajťáků" na městech projevuje zvláštní zášť k čemukoliv, čemu firmy říkají portál občana právě na základě velmi nízkých čísel, která portály generují. Divím se. Je to jako, kdybych chtěl ESHOP na buráky, který mi prodá firma, jež dělá antivir. Když připojím ESHOP k ekonomice a skladu plnému buráků, otevřu si víno a budu čekat na prvního zákazníka. Google analytics mi budou hlásit desítky zákazníků, kteří na moje stránky zamířili ... omylem. Po půl roce neprodám ani jeden oříšek. Co udělám? Zaplatím podporu na další půlrok a budu dál čekat? Přesně tak se mnohá města totiž chovají. Co přesně dělají špatně? Je to hloupé říct, ale skoro všechno. Ve výsledku mají na svém webu odkaz portál občana a na portále občana MV ČR dlaždici. Kde je ale e-government? Nikde. Vůbec nikde.

A jak to dělají jinde?

Podívejme se do Dánska. Na mnoha webech dánských měst najdeme odkazy do portálových řešení. Najdeme tam formuláře? Ne. Rozhodně ne. E-**government v Dánsku není o formulářích, kalamářích a razítkách, byť elektronických. Je o službách pro občany.** Je o snaze pomáhat a nabízet řešení. 90 % českých portálů je založeno na formulářích, které je příliš obtížné vyplnit i pro certifikovaného testera, natož pro otce, který přijde po prohraném fotbalovém zápase domů a zjistí, že musí s dětmi udělat úkoly, uvařit večeři a přihlásit Rexe na město. Až se někdy k půlnoci přihlásí do portálu občana a načte se mu formulář přihlášení psa s 30 kolonkami, z nichž je polovina označena slovy, která vidí poprvé, zakleje a půjde spát do obýváku. Za trest. Jak tomu předejít? Vraťme se do Dánska. V portále občana tam často najdeme životní situace. Ale ne ty z dílny MV ČR, ale jednoduché, máloslovné návody, které nabízejí mraky služeb. **Infografika Vás navede, jak zaplatit psa, jak jej přihlásit ve 2 krocích, kde jsou ve městě parky na venčení psů, cvičiště a kde najdu ty správné pytlíky.** Města totiž zdaleka neřeší jen český svatý grál úplného elektronického podání, ale především to, jak majiteli pejska zlepšit život ve městě.

Dalším příkladem z praxe je životní situace stěhování. Tu v českých portálech nenajdete. Přitom je to zcela běžná věc. Chci se přestěhovat do jiného města a na portále nového sídla si najdu všechny životní situace, které budu řešit. Stěhovací služby. Přihlášení dítěte do školky či školy. Kroužky, které nabízejí příspěvkové organizace města. Komunitní skupiny, abychom do nové čtvrti rychle zapadli, a další a další věci. **Ve výsledku máte dojem, že o Vás město stojí. A to je ve zkratce pocit, který bych strašně rád jako občan ve svém městě cítil. Nu, a to by měl být cíl e-governmentu.**

Dalším vodítkem, které nám pomůže oddělit dobré služby od špatných, je pohled Finska. V argumentaci kolem portálů se můžeme setkat s přepočtem nákladů na jednu provedenou elektronickou platbu. Je to relevantní pohled, nicméně okrajový. Ve Finsku prosadili metriku, která měří, kolik času, této čím dál víc vzácnější veličiny, občanovi



elektronická služba uspoří. Číslo této úspory se musí stát hlavní metrikou e-governmentu města. Zásadní totiž je, že portál občana není agendový systém, i když tak v mnohých řešení vypadá.

A jak to uděláme my?

My bychom měli v první řadě přemýšlet a strategicky plánovat. Jakou službu naše město nabídne občanovi jako první. A jakou jako druhou. A třetí. Tu až napřesrok. Spočítat si, kolik to bude stát na základě cenového průzkumu, který si není nutné nechat zpracovat externí firmou. Na základě takové rozvahy vypracovat plán realizace portálu občana, ve kterém je hlavní kapitola to, čeho chceme dosáhnout. Jakých čísel. Kolik lidí bude navštěvovat životní situace, kolik elektronických plateb provedou. Pak je možné spočítat, kolik času občanům možná ušetříme a zajásat, že pro ně město konečně něco udělá i v elektronickém světě. Zároveň si tak nastavíme i indikátory, které můžeme sledovat a vyhodnocovat, přičemž není od věci se občanů na služby sem tam zeptat třeba na sociálních sítích nebo na přepážkách.

Pokud má město plán elektronických služeb na 2 roky, je možné připravit veřejnou zakázku a připravit integrace a data. **Během léta 2022 by se měl otevřít dotační titul v integrovaném regionálním operačním programu. Minimálně ¾ ceny portálu tak lze získat zpátky z Evropy.** Spojením výhodného financování a plánu elektronických služeb lze získat velmi rychle první elektronické služby města, které budou opravdu využívány. S chutí i pocitem, že jsme si jen neodškrtli naplnění moderních slovíček, ale že jsme taky něco udělali pro občany.

Michal Karvánek
konzultant pro veřejnou správu MARBES
Chcete si popovídat o elektronických službách ve Vašem městě?
Kontakt pro bezplatnou konzultaci:
michal.karvanek@marbes.cz.

MARBES

Elektronická komunikace s občany roste

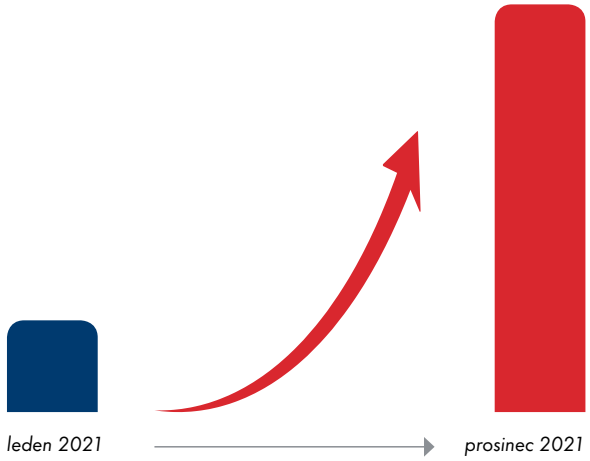
Zavedení bankovní identity, informační kampaň, ale možná i období pandemie spojené s karanténami znamenaly nárůst využití portálů, které občanům zprostředkovávají digitální služby. Nejpatrnější je to na státním Portálu občana.

Trojnásobný nárůst celkového počtu přihlášení

Podle informací Ministerstva vnitra evidoval Portál občana k 1. lednu 2021 celkem 385 000 přihlášení, na konci roku už 1 580 841 přihlášení. To znamená více než ztrojnásobení počtu přístupů za jediný rok.

Nárůst počtu nových uživatelů

Za období od 1. 1. 2021 do 31. 12. 2021 byl také zaznamenán nárůst nových uživatelů o 251 675. K prvnímu lednu minulého roku to bylo 72 200 registrovaných uživatelů, na konci roku už více než 320 tisíc.



Digitální služby portálu

Z cca 400 služeb, které portál nabízí či zprostředkovává, je nejžádanější výpis z Rejstříku trestů pro fyzické osoby (48 236 žádostí v roce 2021). Výrazný zájem je dále např. o výpis ze živnostenského rejstříku (18 642 elektronických výpisů v roce 2021), výpis z bodového hodnocení řidiče (16 000 v roce 2021) nebo o elektronickou žádost o nový řidičský průkaz (16 000 žádostí v roce 2021 od spuštění služby 1. června 2021). Jednoznačně se projevil nárůst uživatelů Portálu občana po přidání možnosti přihlášení bankovní identitou.

Dá se říct, že touto cestou se dnes přihlašují tři čtvrtiny všech uživatelů portálu. Bankovní identita tak v pozici vystřídala hlavní způsob přihlášení přes datové schránky, které měly ještě v roce 2020 podíl 56 % na přihlášení.

Výpis z Rejstříku trestů pro fyz. osoby

48 236 žádostí

Výpis ze živnost. rejstříku

18 642 výpisů

Výpis z bodového hodnocení řidiče

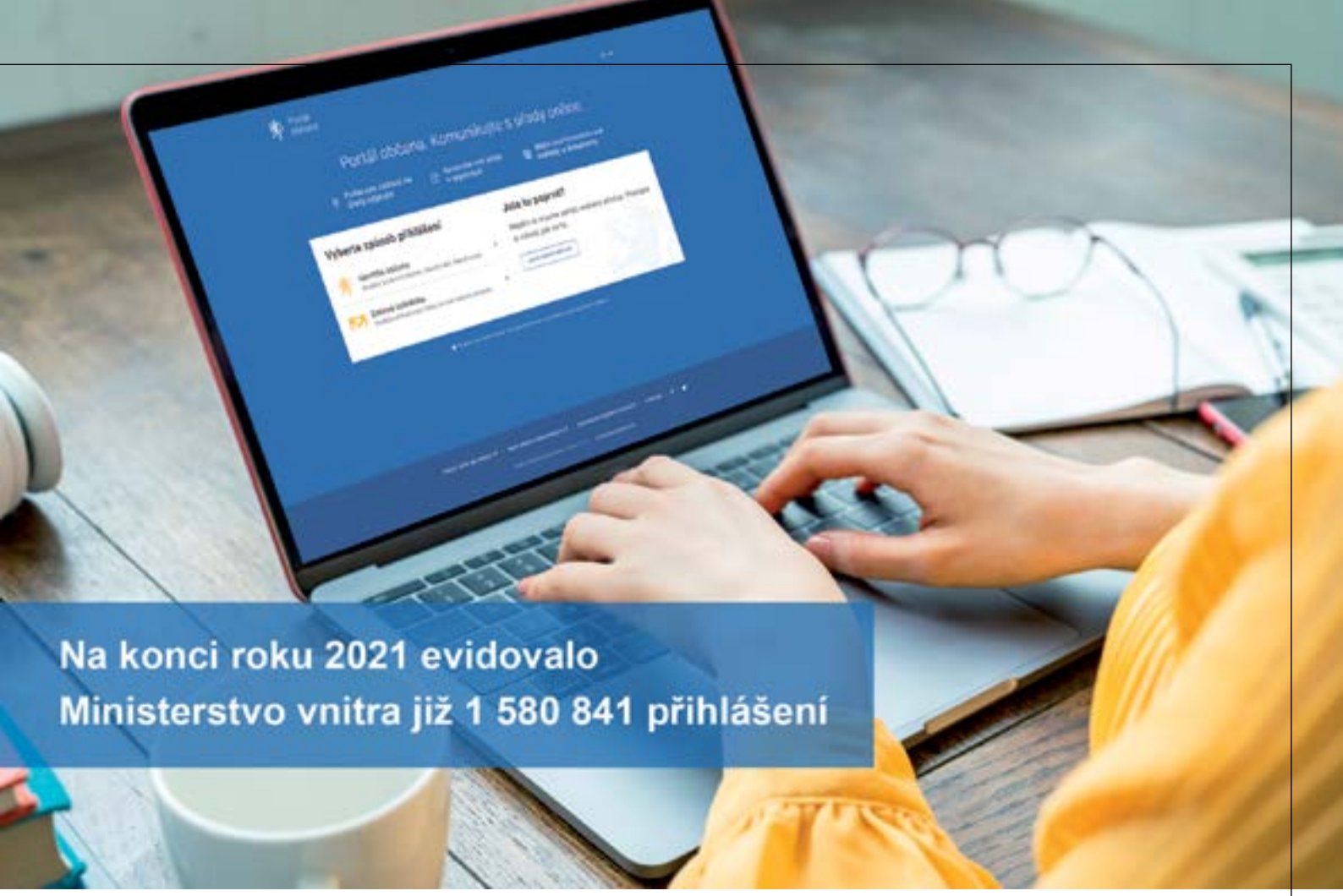
16 000 výpisů

Elektronická žádost o nový řidičský průkaz

16 000 výpisů

Územně samosprávní celky

Zvýšený zájem o digitální služby registrovaly v uplynulém roce také územně samosprávní celky. Nárůst přihlášených uživatelů do svého portálu občana zaznamenali například ve Znojmě, a to z 494 na 688, tedy o téměř o 40 procent. V Prostějově počet přihlášených uživatelů dosáhl v roce 2021 na téměř 500 z původních 324, zvýšil se tedy o více než 50 procent. Nejčastějším úkonem, pro který prostějovští občané portál využili, byla žádost o dotaci. Právě pro řešení grantů a dotací se nabízí využití tzv. zastoupení právnických osob, které poskytuje Portál občana Gordic. Za právnickou osobu vždy musí jednat k tomu určená či zmocněná fyzická osoba. Po založení právnické osoby v portálu získá možnost při dalším přihlášení zvolit, zda chce jednat za sebe či za přiřazenou organizaci.



I poskytování podpory sportovním klubům nebo zájmovým sdružením na území města či kraje jde snadno digitalizovat. A je zde určitě velký potenciál, protože třeba bývalá okresní města většinou evidují podobných žádostí o dotace či granty několik set. Ale zajímavých služeb může být na portálu více. V Třešti na Jihlavsku naleznete v detailu poplatku za komunální odpad kromě historie plateb a napojených poplatníků také přehled svozu popelnic s datem a identifikátorem vaší odpadní nádoby.

Možnost digitální úhrady poplatků

Tím jsme se na závěr dostali k oblasti, která je pro atraktivitu portálu občana každé organizace zásadní, a to k možnosti úhrad poplatků. Její význam si uvědomili například ve městě Veselí nad Moravou, kde vedle zajištění elektronického podání digitálních formulářů pro řešení životních situací občanů požadovali i možnost plateb pomocí QR kódu či platební brány. Aby občany motivovali, zavedli 20 % slevu u platby za komunální odpad pro ty, kteří se do portálu registrují a platbu provedou elektronicky. Ukázalo se to jako dobrý krok. Přes platební bránu bylo za rok 2020 provedeno 304 plateb, v roce 2021 už to bylo 522. Veselí nad Moravou i díky tomu patří k premiantům co se týče procenta občanů zapojených do digitální komunikace s městem.

Výše uvedené může sloužit i jako náměty pro další města a obce. Jak se ukazuje, v současnosti už není z hlediska poskytování digitálních služeb problém v legislativě ani v technologiích. A nechybí ani erudice občanů jako jejich konzumentů. Digitální identitu jsme masivně používali například v souvislosti s očkováním a testováním na covid-19 nebo při sčítání lidu v roce 2021. Existují však stále rezervy v nabídce digitálních služeb, které by lidi zajímaly. A nedostatečná je pořád i jejich dostupnost a propagace. Není výjimkou, že město schovává svůj portál občana někde hluboko ve struktuře webu. Přitom by to mělo být naopak, občan by měl hned na první pohled vidět, kde se může přihlásit a co vše může digitálně vyřídit. Věřme, že i v tomto dojde ke zlepšení a veřejné digitální služby budeme využívat již brzy se stejnou samozřejmostí jako nákup v e-shopu.

GORDIC

Služba vytváření kvalifikovaných elektronických podpisů na dálku I.CA RemoteSign

V současné době rostou nároky na zjednodušení a zrychlení procesů založených na takových typech dokumentů, které vyžadují jednoznačnou autorizaci osobou nebo i více osobami prostřednictvím jejich podpisu. Řešením je elektronizace agend, a tedy i vytváření elektronických dokumentů, které však musí plnohodnotně nahradit dokumenty fyzické, a to včetně podpisů. Jedině kvalifikovaný elektronický podpis je ekvivalentem vlastnoručního podpisu a pro jeho vytváření je obvyklé, aby podepisující osoba měla k dispozici bezpečné zařízení – kvalifikovaný prostředek pro vytváření elektronického podpisu (QSCD) v podobě čipové karty nebo USB tokenu.

Ne vždy je takové řešení pro uživatele vhodné a jednoduše použitelné. První certifikační autorita, a.s., (I.CA) provozuje již pro několik komerčních subjektů službu elektronického podepisování na dálku pod obchodním názvem I.CA RemoteSign.

Uživatel této služby nemá vlastní bezpečné zařízení – QESCD, ale využívá vzdáleného přístupu k bezpečnému zařízení, které je spravováno kvalifikovaným poskytovatelem služeb vytvářejících důvěru, a to plně v souladu s požadavky Nařízení EU 910/2014 – eIDAS (články 51 a 52).

Služba I.CA RemoteSign umožňuje vytváření kvalifikovaného elektronického podpisu na mobilních zařízeních (mobilní telefony a tablety). Uživatel má vždy k dispozici speciální aplikaci, kterou využívá pro přijímání požadavků a vytváření kvalifikovaného elektronického podpisu. V současnosti jsou v rámci služby podporována mobilní zařízení s operačním systémem Android nebo iOS. Nově také připravujeme aplikaci pro vytváření elektronického podpisu na dálku pro další typy zařízení (PC/NB) na platformě Windows. A pro nižší objemy dokumentů zasílaných k podpisu bude uživatelům služby již brzy k dispozici také serverová aplikace pro manuální zasílání dokumentů, kterou jistě využijí menší poskytovatelé služeb nebo úřady a instituce. Tato aplikace bude vhodná i pro vnitřní agendy typu personální, schvalování došlých faktur apod.

Aktivace služby, správa identit

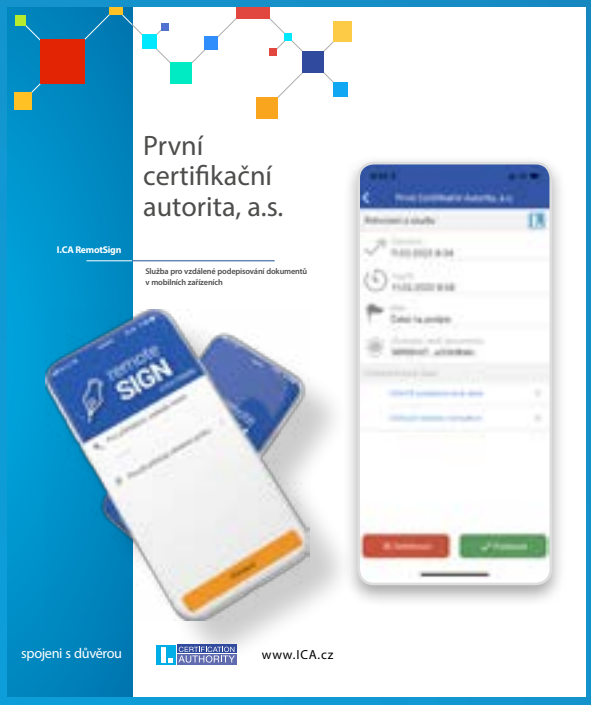
Aktivace služby probíhá na obchodním místě I.CA nebo na kontaktních místech samotných poskytovatelů služeb. Zde je provedeno ověření totožnosti uživatele (žadatele o službu) a jeho registrace. Po provedení registrace získá uživatel podklady pro aktivaci služby, tzv. aktivační obálku, která (jako jediná) obsahuje potřebné „tajemství" pro zpřístupnění práce s privátním klíčem, k němuž byl vydán příslušný kvalifikovaný certifikát. Poté si uživatel stáhne aplikaci I.CA RemoteSign a pro její aktivaci použije kód z aktivační obálky, kterou získal při registraci. Během procesu aktivace dochází ke generování prvního párů klíčů pro danou identitu a vydání prvotního kvalifikovaného certifikátu. Po aktivaci aplikace je služba okamžitě dostupná.

Podepisování dokumentů

1. Poskytovatel služeb vytvoří požadavek na podpis dokumentu.
2. Požadavek je vložen do systému I.CA RemoteSign (RSiCon) na straně poskytovatele služeb.
3. Systém I.CA RemoteSign odešle notifikaci o novém požadavku k podpisu příslušnému uživateli.
4. Uživatel v aplikaci I.CA RemoteSign zaslaný požadavek podepíše.
5. Podepsaný požadavek je předán a uložen na do systému I.CA RemoteSign na straně poskytovatele služeb.
6. Poskytovatel služeb si převezme podepsaný požadavek a provede jeho zpracování.

Technické řešení

Poskytovatel služeb vkládá požadavky k podpisu prostřednictvím komponenty RSiCon, která je integrována v jeho interním systému, případně manuálně prostřednictvím aplikace I.CA RS Sender. Na základě takového požadavku dojde v komponentě RSiCon k činnosti procesů nutných k realizaci podpisu, výpočet hash, vytvoření náhledu dokumentu a přes I.CA RemoteSign Server, provozovaný v prostředí I.CA, jsou zašifrovaná data zaslána na všechna aktivní mobilní zařízení daného uživatele formou push notifikace. Po jejím otevření dojde ke spuštění mobilní aplikace I.CA RemoteSign. V aplikaci se uživatel autentizuje heslem, případně biometricky otiskem prstu nebo obrazem obličeje



a zobrazí se mu seznam čekajících požadavků k podpisu. Uživatel si může u jednotlivých dokumentů zobrazit detailní informace. Každý požadavek má definovanou platnost, což je časový údaj zadaný poskytovatelem služeb. Po jeho uplynutí uživatel nemá dále možnost dokument podepsat. Pokud se uživatel rozhodne podepsat, zadá heslo a následně se vytvoří kvalifikovaný elektronický podpis hash podepisovaných dat. Po podpisu dochází k tzv. notifikaci systému poskytovatele služeb, který je tak informován o změně stavu podpisové transakce. Následně systém poskytovatele služeb volá prostřednictvím komponenty RSiCon systém I.CA RemoteSign, dojde ke stažení kryptogramu a následnému sestavení kompletního podepsaného dokumentu. Dokument je vrácen volajícímu systému poskytovatele služeb a je možné s ním nakládat jako s jakýmkoliv jiným elektronicky podepsaným dokumentem. Pokud je pro zasílání používána aplikace I.CA RS Sender, je podepsaný dokument k dispozici pro manuální zpracování.

Bezpečnost

- Kvalifikovaný elektronický podpis je vytvářen na certifikovaném HSM (QSCD) ve správě kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Veškerá komunikace mezi mobilním zařízením uživatele a službou I.CA RemoteSign je šifrována speciálně vytvořeným protokolem.
- Data předávaná do systému I.CA RemoteSign nezahrnují obsah podepisovaného dokumentu.
- Náhled dokumentu v PDF formátu nebo odkaz na stažení podepisovaných dat jsou předávány v zašifrované podobě. K jejich dešifrování může dojít až na koncovém zařízení podepisujícího uživatele.
- V rámci procesu aktivace prvního zařízení uživatele dojde k úpravě zabezpečení přístupu k privátnímu klíči takovým způsobem, že nadále již k přístupu nepostačuje obsah aktivační obálky, ale je nutná kombinace tajemství uloženého v zařízení uživatele (generovaného v rámci aktivace) a hesla pro podpis na dálku, jež si uživatel během aktivace zvolil.
- Během procesu podpisu neopouští privátní klíč k certifikátu bezpečné prostředí HSM modulu, pouze dojde v zařízení uživatele k sestavení tzv. SAD (Signature Activation Data), která obsahují autorizaci použití klíče uživatele na konkrétní hash hodnotu. Tyto SAD jsou zaslány do HSM modulu, kde dojde k ověření jejich správnosti, a po úspěšném ověření je proveden podpis pomocí privátního klíče uživatele nad příslušným hashem. Tato vzniklá hodnota kryptogramu je pak následně použita pro sestavení celé struktury elektronického podpisu dle příslušných norem.

Závěr

I.CA RemoteSign je plně v souladu s platnou legislativou a umožňuje podepisovat dokumenty uživatelům chytrých telefonů, tabletů i PC/NB kvalifikovaným elektronickým podpisem s možností připojení kvalifikovaných časových razítek. Zároveň naplňuje i náročné požadavky uživatelů na možnost rychle a snadno podepisovat dokumenty s využitím mobilních telefonů nebo tabletů, které mají obvykle uživatelé u sebe nejen v kancelářích, ale i na cestách nebo doma. Služba je využitelná různými poskytovateli služeb, jako jsou banky, pojišťovny, dodavatelé energií a řada dalších obchodních subjektů a rovněž orgánů veřejné moci.

Roman Mašata, vedoucí projektu
a key account manažer,
První certifikační autorita, a.s.

Jak FortiSOAR pomáhá SOC centrům

Neustále se rozšiřující digitální útočná plocha ztěžuje organizacím proaktivní správu jejich síťové bezpečnosti. To vede mnohé podniky k nasazení dodatečných bezpečnostních nástrojů s cílem posílit schopnost zabezpečení nových prostředí a zařízení. Využívání řešení od různých dodavatelů však decentralizuje síťové operace, zatímco používání statických bezpečnostních zařízení k zabezpečení dynamických síťových prostředí může mít za následek vytvoření kritických mezer v bezpečnosti. S rostoucím nedostatkem kvalifikovaných odborníků v oblasti kybernetické bezpečnosti mají IT týmy také problémy s budováním a údržbou bezpečnostních systémů, které by dokázaly udržet krok se současnými sofistikovanými hrozbami. Tyto výzvy vedou k využívání nástrojů SOAR k zefektivnění bezpečnostních operací a zkrácení doby odezvy na incidenty.

Jakým způsobem může SOAR pomoci týmům SOC aktivovat správu hrozeb

Práce na identifikaci výstrah z různých zdrojů pro týmy bezpečnostních operačních center (SOC) není vůbec jednoduchým úkolem. Množství falešných upozornění v kombinaci s manuálním úsilím potřebným k ověření jejich legitimnosti zpomaluje čas odezvy na incidenty, což reálně znamená, že identifikace a zabránění narušení zabere delší dobu. Právě tyto faktory spolu se současným nedostatkem kvalifikované pracovní síly v oblasti kybernetické bezpečnosti způsobují, že mnohé týmy SOC jsou přetíženy a nejsou schopny efektivně identifikovat a napravit hrozby ve svých sítích.

„Pomocí řešení SOAR (bezpečnostní orchestrace, automatizace a odezva) mohou týmy SOC zefektivnit svou bezpečnostní reakci a zároveň sjednotit své operace. Integrace řešení dále poskytuje týmům SOC možnost vytvořit centralizovanou bezpečnostní platformu, která umožňuje koordinovanou snahu v oblasti kybernetické bezpečnosti založenou na použitelném zpravodajství o hrozbách (threat intelligence). Kromě toho tento model dokáže optimalizovat interní procesy upřednostňováním strategických výstrah, snížením pracovního zatížení členů týmu a zlepšením viditelnosti hrozeb," uvádí Ondřej Šťáhlavský, Sr. Regional Director CEE ze společnosti Fortinet.

Výzvy, kterým čelí týmy SOC center

V důsledku nadměrného počtu výstrah v bezpečnostních operačních centrech (SOC) může vzniknout několik problémů, včetně následujících.

Zabezpečení a udržení talentovaných pracovníků

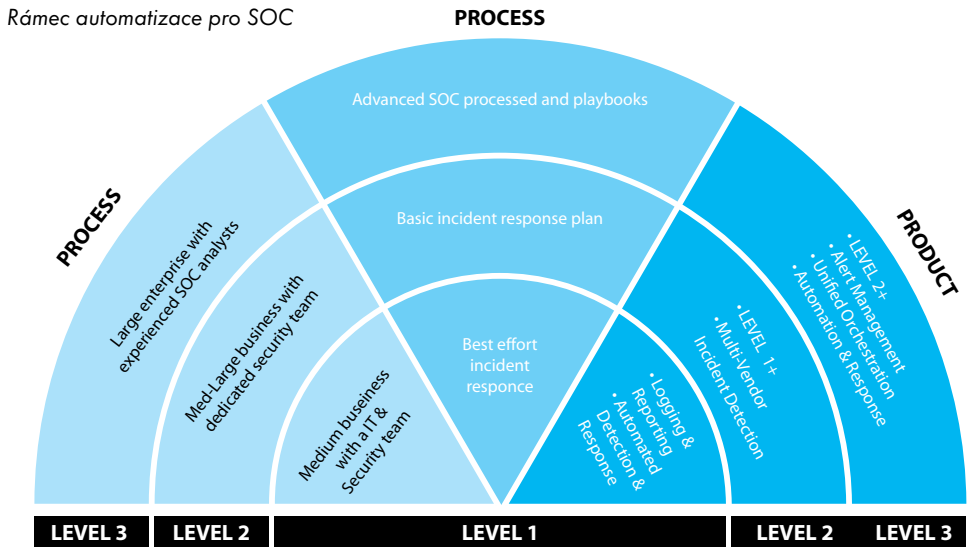
Většina (64 %) každodenních úkolů vykonávaných provozním personálem SOC je manuálních, repetitivních a zaměřených na používání dezintegrovaných nástrojů. Tyto faktory v kombinaci se zdánlivě neustálým přílivem informací, často v nepravidelných hodinách, mohou ztížit udržení personálu SOC.

Odezva na incident

Dnešní technologie využívané při kybernetických útocích dokáží úspěšně proniknout do sítě během několika vteřin, přičemž často využívají nově nasazené vektory útoků. A protože kyberzločinci začínají využívat pokročilé únikové techniky a experimentují s využitím automatizace a umělé inteligence při realizaci útoků, manuální reakce již není adekvátní volbou k udržení bezpečnosti sítí. Když k tomu přidáte aspekt nadměrného počtu varování, objem údajů generovaných rostoucím počtem zařízení a nedostatek kvalifikované pracovní síly, je jasné, že mnohé týmy SOC nejsou dostatečně vybaveny pro zvládání pokročilých kybernetických hrozeb.

Chybějící centralizovaná bezpečnostní infrastruktura

Nástroje, které používají Network Operations Center (NOC) a pracovníci SOC k vykonávání své práce, obvykle nejsou navrženy tak, aby navzájem spolupracovaly. Tento nedostatek soudržnosti zvyšuje pravděpodobnost přehlédnutí problému při identifikaci a řízení hrozeb.



Sjednocený „case management"

Odezva na hrozby často zahrnuje několik týmů pracujících na různých změnách, a dokonce i v různých časových pásmech, což ztěžuje spolupráci. Bez jednotného integračního bodu pro case management a digitálně založené korelace a koordinované reakce se zvyšuje pravděpodobnost, že hrozby budou řízeny nesprávně nebo nebudou odhaleny vůbec.

Jakým způsobem FortiSOAR optimalizuje operace SOC u partnerů

FortiSOAR je agnostickým řešením, které umožňuje týmům bezpečnostních operací zlepšit jejich síťové operace vytvořením vlastního automatizovaného rámce, který centralizuje bezpečnostní možnosti jejich organizace. Výsledkem je, že týmy SOC mohou sjednotit a standardizovat své procesy, čímž se zkrátí časy odezvy a odstraní se nadměrný počet varování. Kromě toho se viditelnost získaná pomocí FortiSOAR promítá do strategičtějších upozornění v rámci kybernetické bezpečnosti, což umožňuje týmům SOC přizpůsobit a optimalizovat své bezpečnostní postupy podle potřeby.

Jak je možné využít FortiSOAR k optimalizaci svých operací SOC, a tím poskytnout zvýšenou hodnotu zákazníkům?

Zvýšená přesnost a konzistentnost odezvy

Manuální správa různých bodových řešení brání vyšetřování výstrah a přináší příležitosti pro přehlédnutí problémů a chyb. Větší a pokročilé týmy SOC těží z řešení FortiSOAR nejvíce, jelikož řešení také využívá funkce nabízené FortiAnalyzerem a FortiSIEM ke zlepšení viditelnosti a dokáže automatizovat jednoduché úkoly SOC, jako je příjem upozornění a přiřazení úkolů. S úrovní pokročilé automatizace, kterou FortiSOAR nabízí, mohou týmy SOC urychlit svoji reakci na hrozby a zároveň omezit manuální chyby a reagovat rychlostí stroje díky automatizovaným příručkám.

Kolaborativní „threat management"

Odstraněním manuálních úkolů mohou týmy SOC lépe řídit své zdroje, včetně času a práce zaměstnanců.

„FortiSOAR také umožňuje zákazníkům spolupracovat na správě případů napříč pracovními změnami. Workflow každého člena týmu je dokumentována a je kdykoli přístupná, aby zaměstnanci, kteří pracují na různé směny, mohli koordinovat své úsilí. Tato funkce také zajišťuje, že se neztratí důležité poznatky, když zaměstnanec změní tým nebo opustí organizaci," dodává Ondřej Šťáhlavský, Sr. Regional Director CEE společnosti Fortinet.

FORTINET

Autor: společnost Fortinet

Penetrační testování: ověřte odolnost, než bude pozdě

Ve všech fázích vývoje aplikací platformy GINIS klademe velký důraz na kybernetickou bezpečnost. I přesto zákazníkům doporučujeme a nabízíme penetrační testování. Pokud vás napadá, že to jde tak trochu proti sobě, rád vás vyvedu z nemalého omylu.

Pořízení nejbezpečnějších vchodových dveří domu také není všespásné, pokud máte nekvalitní okna či bezpečnostní systém, chybně řešené větrací šachty, přístupný zadní vchod nebo „zfušované" usazení samotných dveří. A i kdybyste tohle všechno bravurně podchytili, může nebezpečí číhat v procesním nastavení – děti mohou půjčit klíč od vchodu pochybnému kamarádovi nebo si je snad kamarád může „půjčit" sám během hodiny tělocviku. Takhle nějak to funguje i ve světě IT. Kompletní výčet slabých míst informačního systému a bezpečnostních rizik lze získat až testováním v prostředí organizace. A přesně k tomu slouží penetrační testy.

Co je to penetrační test

Jedná se o podrobnou a komplexní analýzu zabezpečení infrastruktury, systémů i samotných aplikací, využívající zátěžové a další formy testů, včetně simulací principů potenciálních útoků zevnitř i z externího prostředí, tedy z internetu. Aplikace jsou v našem pojetí podrobeny jak manuálnímu, tak i automatizovanému testování v režimu „black box". Výstupem je nejen report hrozeb a nedostatků, ale i soubor návrhů opatření k eliminaci či minimalizaci existujících rizik. GORDIC zajišťuje takové testování většinou v souvislosti s nasazením či rozvojem platformy GINIS u konkrétních organizací, dovedeme však tento typ služeb zprostředkovat i pro ostatní využívané aplikace jiných dodavatelů. Samozřejmě za předpokladu, že nám organizace a dodavatelé zajistí potřebné přístupy.

Testování v praxi

U webových aplikací (které jsou jednoznačným trendem současnosti) je po důkladném testování samotné aplikace klíčové ověřit i to, zda je možné ovlivňovat přidělená anonymní oprávnění a narušit tak integritu, dostupnost a samotnou důvěryhodnost aplikace, případně kompromitovat data. Testy probíhají podle metodiky OWASP. Ta je doplněna dalšími postupy, které zkušení testeři vyhod-

notí jako vhodné a relevantní pro daný typ aplikace či nastavení systému. Proces tak obvykle zahrnuje i testování sítě a jejího nastavení, ochrany webu (firewall), protokolů, šifrování, ochrany dat i další kroky vycházející z metodických doporučení NÚKIB a legislativních předpisů (zejména zákon a vyhláška o kybernetické bezpečnosti).

Nedokonalý výsledek není ostuda

Viry a IT hrozby se neustále vyvíjejí, infrastruktura zastarává, dodržování procesů mnohdy v čase slábne. I pro nás tvoří výsledky penetračních testů cenný podklad pro ladění námi vyvíjených aplikací, které tak lépe dovedou čelit aktuálním hrozbám. Poslední takovou optimalizaci jsme prováděli u řešení Portálu občana na základě testování v prostředí statutárního města Přerova. Rozhodně by ničemu nepomohlo rizika, ač třeba minimální, bagatelizovat. Řešení máme i pro případ, kdy by vedení organizace mělo obavy z testování firmou, která je zároveň dodavatelem samotného řešení. Umíme zprostředkovat penetrační testování externí firmou, která taktéž disponuje veškerou certifikací, profesionalitou a zkušenostmi v oboru.

Více kol, více bezpečí

Opakování není pouze matkou moudrosti, ale i bezpečnosti. Nalijme si čistého vína – pouze málo organizací má IT infrastrukturu, procesy a přístupy dokonale zabezpečené a připravené na to, aby nová implementace nějakou tu skulinku nevytvořila či neodkryla. Po realizaci nápravných kroků mezer, odhalených testem, je žádoucí testování zopakovat pro zjištění, zda se opatření neminulo účinkem nebo nevytvořilo jiný nedostatek.

Data a znovu data

Úskalím organizací veřejné správy je práce s aktuálně asi nejcennější komoditou – s daty. Bezpečnost se tak stává nutností a liknavý přístup cestou do pekel. Pekel v podobě ztráty či krádeže dat nebo paralýze úřadu a nákladného návratu do normálu. Penetrační testování by proto nemělo chybět v mozaice preventivních bezpečnostních opatření organizace jakékoliv velikosti.

Ing. Michal Tausch
ředitel odboru podpora obchodu,
Gordic spol. s r.o.

GORDIC

Otevřená data – nástroj sdílení dat pro výkon veřejné správy

Pro naplnění myšlenky eGovernmentu jsou důležité moderní elektronické nástroje, avšak v takovém prostředí, jako je veřejná správa, která provozuje několik tisíc informačních systémů, je stejně důležitý i způsob, jakým všechny systémy vzájemně sdílejí data veřejné správy, a s ním související pravidla a standardy.

Otevřená data se stala svými principy, snadností používání a orientací na otevřené standardy téměř universální integrační platformou pro různorodé zdroje dat. Výrazně podporují architekturu systémů, ve kterých jsou data primárními a trvalými aktivy, kolem kterých se odehrává vše ostatní. Datový model takových systémů se stává trvalejší, předchází implementaci jakýchkoliv aplikací a zůstává platný i poté, když je jedna aplikace nahrazena aplikací jinou. Data jsou centrem systému. Podobnost takové architektury se stávajícím modelem veřejné správy je zcela na místě, a tak je zcela opodstatněná snaha mít k dispozici více prostředků a nástrojů, zajišťujících sdílení veřejných dat mezi orgány veřejné správy ČR. Jedním z těchto nástrojů se stala i otevřená data, která jsou v informační koncepci ČR zahrnuta mezi stavební kameny moderní architektury veřejné správy.

Orgány veřejné moci (OVM) a soukromoprávní uživatelé údajů (SPUÚ) používají při výkonu svých agend údaje vedené v základních registrech, údaje vedené v agendových informačních systémech a případně i další údaje. Pro zajištění efektivní veřejné správy je nutné, aby OVM a SPUÚ měly pro sdílení údajů k dispozici jasně definovanou sadu metod a nástrojů ukotvenou v celkové architektuře eGovernmentu, nezávislou na jednotlivých informačních systémech VS.

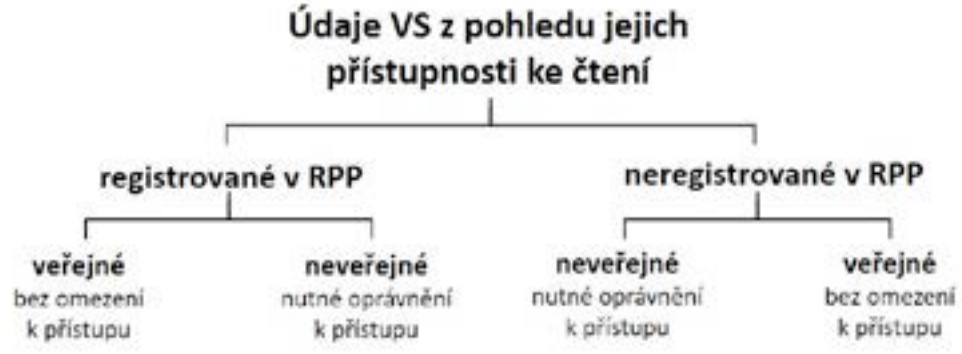
Údaje veřejné správy jsou údaje evidované jednotlivými OVM v jejich informačních systémech. **Z pohledu sdílení údajů je důležité jejich členění na:**

- údaje evidované v registru práv a povinností (RPP) v rámci ohlášení agendy (dále jen registrované údaje) a ostatní údaje (dále jen neregistrované údaje);
- veřejné a neveřejné údaje.

Jako veřejné údaje jsou označeny údaje, které může kdokoliv číst bez omezení přístupu. Omezení veřejnosti údajů vychází primárně ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a to zejména z ochrany utajovaných informací, ochrany obchodního tajemství, ochrany důvěrnosti majetkových poměrů, ochrany osobních údajů a dalších omezení práva na informace dle tohoto zákona. Sekundárně veřejnost údajů upravují i další speciální právní předpisy.

Neveřejné údaje jsou ty, pro jejichž čtení jsou nutná oprávnění k přístupu.

Z uvedeného vyplývá následující klasifikace údajů veřejné správy (obr. 1).



Obr. 1 Klasifikace údajů veřejné správy

Myšlenkou tzv. eGovernmentu je správa věcí veřejných využitím moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější.
(citace: web MV ČR, odbor eGovernmentu)

Registrované údaje jsou tedy údaje, o jejichž existenci explicitně informuje OVM jako ohlašovatel agendy prostřednictvím evidence v RPP. OVM je nabízí ke sdílení tím, že je poskytuje do stávajícího propojeného datového fondu (PPDF) a nově také do veřejného datového fondu (VDF) prostřednictvím referenčního rozhraní.

Neregistrované údaje jsou všechny ostatní údaje. Jejich správce musí vést v patrnosti, že nelze obejít zveřejňování údajů do referenčního rozhraní tím, že je nebude registrovat do RPP, a musí neexistenci evidence údaje v RPP obhájit.

PPDF slouží primárně ke sdílení registrovaných **neveřejných údajů** mezi jednotlivými OVM a ke zpřístupnění těchto údajů jednotlivým SPUÚ pro účely výkonu jejich agend na základě oprávnění pro čtení nebo pro zápis evidovaných v RPP.

VDF slouží ke sdílení **veřejných registrovaných údajů** mezi jednotlivými OVM a ke zpřístupnění těchto údajů jednotlivým SPUÚ v podobě otevřených dat dle § 3 odst. 11 zákona o svobodném přístupu k informacím bez nutnosti oprávnění pro jejich čtení v evidenci RPP.

Veřejný datový fond je ustanoven a definován v Informační koncepci ČR (IKČR) v dílčím cíli 5.10 jako součást eGovernmentu VS ČR:

„Veřejný datový fond tvořený publikovanými veřejnými údaji veřejné správy je základní metodou pro sdílení veřejných informací mezi veřejnoprávními subjekty navzájem i pro sdílení veřejných údajů mezi veřejnoprávní a soukromoprávní sférou v ČR. Veřejný datový fond se od pouhé publikace automatizovaně čitelných otevřených dat posune též k publikaci právně závazných, platných a pravidelně aktualizovaných datových sad s jasně definovanou zodpovědností OVS za takové sady."

V definici VDF je doslovně uvedeno, že se jedná o metodu sdílení informací, což znamená, že VDF představuje tematickou oblast (podobně jako v případě PPDF), která zahrnuje téměř všechny ISVS s jejich daty, způsoby jejich vzájemné komunikace, související standardy, pravidla a doporučené postupy pro zajištění vzájemného sdílení dat. Z těchto důvodů také není VDF jako pojem v legislativě explicitně uveden, ale je rozprostřen (vnořen) do ustanovení v relevantních zákonech. Jedná se zejména o zákon č. 111/2009 Sb., o základních registrech, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, a zákon č. 365/2000 Sb., o informačních systémech veřejné správy.

Obecným výchozím principem, který tvoří základ VDF, je princip P13 eGovernmentu „otevřená data jako standard" (Open Data by Default):

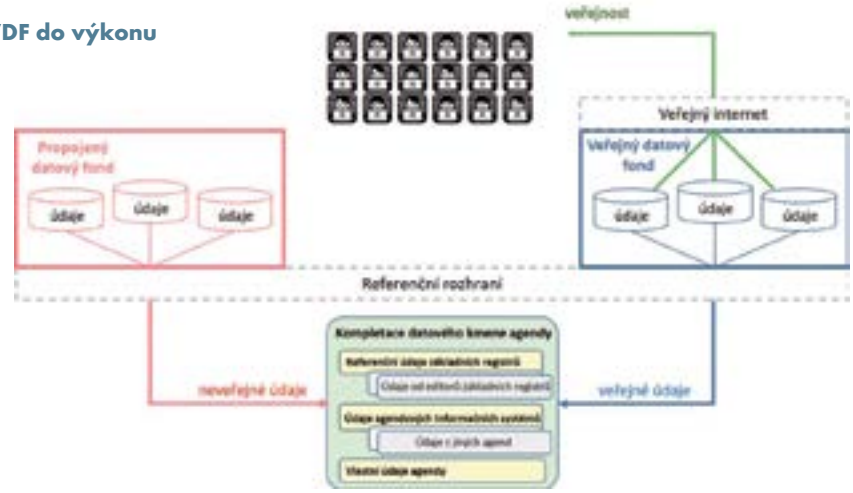
„Veřejné údaje evidované orgány veřejné správy ve spravovaných ISVS musí být zveřejňovány jako otevřená data. Pro neveřejné údaje musí být jako otevřená data zveřejňována jejich anonymizovaná podoba, souhrn nebo statistika. V případě, že orgány veřejné správy sdílejí veřejné údaje (včetně anonymizované podoby neveřejných údajů, souhrnů nebo statistik), musí je sdílet jako otevřená data."

VDF zpřístupňuje veřejné registrované údaje jednotlivým OVM a SPUÚ pro čtení bez omezení přístupu jako otevřená data dle § 3 odst. 11 zákona o svobodném přístupu k informacím, a tedy z podstaty jejich „veřejnosti" jsou přístupné ve stejné otevřené podobě i veřejnosti.

Veřejný datový fond nepředstavuje žádný další konkrétní informační systém VS (ISVS), který by bylo možné popsat jako jeden celek s funkční specifikací, ale komplexní systém zastřešující tematickou oblast nad:

- veřejnými údaji veřejné správy;
- technickou infrastrukturou tvořenou:
  - společnými komponentami, zaměřenými na správu a organizaci zpřístupňovaných údajů – plně zajišťovanými MV ČR,
  - doplňujícími komponentami ISVS, určenými pro zpřístupnění a užívání údajů jednotlivých agend – zajišťovanými jednotlivými organizacemi VS, správci agend, správci ISVS (způsob jejich fyzické realizace není stanoven);
- pravidly a definovanými standardy pro zajištění interoperability sdílených údajů;
- procesy a postupy pro zajištění právní závaznosti, platnosti, aktuálnosti a jasně definovaných zodpovědností za sdílené údaje.

Obr. 2 Zakomponování VDF do výkonu veřejné správy



Obrázek 2 zachycuje zakomponování VDF do výkonu veřejné správy při kompletaci datového kmene prováděné agendy.

Pravidla a standardy zajišťující vlastnosti VDF definované v dílčím cíli 5.10 Informační koncepce ČR vychází ze čtyř základních principů:

- P1 (distribuovanost) – VDF zastřešuje a popisuje skutečné datové zdroje poskytující údaje prostřednictvím referenčního rozhraní a stanovuje pravidla poskytování a čerpání údajů, ale nevynucuje jejich centralizaci na jedno místo;
- P2 (garance) – pro OVM a SPUÚ čerpající údaje z VDF je garantována technická dostupnost a formální správnost (věcná správnost, úplnost, platnost a pravidelná aktualizace) těchto údajů;
- P3 (otevřená data) – údaje přístupné z VDF jsou zpřístupněny jako otevřená data dle § 3 odst. 11 zákona o svobodném přístupu k informacím bez výjimky;
- P4 (interoperabilita) – údaje jsou z VDF zpřístupněny v podobě, která zajišťuje schopnost různých programových vybavení vzájemně si poskytovat služby a efektivně spolupracovat.

Vytvoření plně funkčního VDF a doladění související legislativy si vyžádá delší období, jeho implementace ale již byla zahájena a aktuální stav je následující:

- legislativa – zákon č. 111/2009 Sb. zavádí povinnost označovat registrované údaje jako veřejné nebo neveřejné a jako údaje kódované číselníkem. Pro údaje kódované číselníkem zavádí povinnost používat existující číselníky, příp. zavádět do registru práv a povinností vlastní číselníky, které musí být publikovány jako otevřená data dle otevřené formální normy pro číselníky. Ze spojení se zákonem č. 106/1999 Sb. pak vyplývá, že veřejné údaje musí být publikovány jako otevřená data;
- společná infrastruktura – pro potřeby katalogizace datových sad zpřístupňujících veřejné údaje ve VDF je již připraven Národní katalog otevřených dat, během léta 2022 bude uvedeno do provozu rozšíření registru práv a povinností, ve kterém budou implementovány změny vyplývající ze zákona č. 111/2009 Sb.;
- metodické postupy – během léta 2022 vydá MV ČR metodiku poskytování údajů ve VDF.

V dalším období je pak nutné zajistit především sdílení číselníků a veřejných údajů v podobě otevřených dat prostřednictvím referenčního rozhraní.

Všechny ISVS, které evidují veřejné údaje, budou muset být upraveny tak, aby veškeré v nich vedené veřejné registrované údaje byly publikovány jako data dostupná všem OVM a SPUÚ bez omezení prostřednictvím referenčního rozhraní.

Veřejný datový fond, a tedy v podstatě otevřená data, se tak stávají významnou součástí architektury VS ČR a zcela určitě mají díky svým vlastnostem velký potenciál napomoci k naplnění myšlenky eGovernmentu, aby *„veřejná správa byla k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější"*.

Autoři: Drahomír Chocholatý, Martin Nečaský

Tento článek vznikl v rámci projektu „Rozvoj datových politik v oblasti zlepšování kvality a interoperability dat veřejné správy" OPZ č. CZ.03.4.74/0.0/0.0/15_025/0013983, který zastřešuje odbor hlavního architekta eGovernmentu Ministerstva vnitra ČR.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

iSSS 2022

16.–17.5.22
HradecKrálové

Kongresové centrum **Aldis**

Konference zaměřená na **digitalizaci veřejné správy** a **rozvoj e-governmentu**

24. ročník	**2** denní program	**±150** přednášek	**±80** prezentujících firem a institucí	**±2000** průměrná návštěvnost

Konference se bude věnovat zejména těmto tématům

- Záměry a plány v oblasti eGovernmentu pro aktuální volební období
- Institucionální a kompetenční změny v eGovernmentu – důvody a dopady
- Řízení a rozhodování na základě dat
- Digitální identita a její využití ve fyzickém světě
- Rozvoj komunikační infrastruktury
- Kybernetická bezpečnost a krizové řízení
- Elektronizace zdravotnictví a jeho role (nejen) při pandemii
- Efektivita a snižování nákladů
- Spisové služby a archivace digitálních dokumentů
- Digitalizace specifických oblastí veřejné správy
- Workshopy, panelové diskuse, příklady dobré praxe, populární soutěže

Další informace týkající se upřesněných okruhů témat a koncepce jednotlivých odborných bloků budou postupně zveřejňovány na **www.isss.cz**

pořadatel: TRIADA

spolupořadatel: Kraj Vysočina

spolupracují: Královéhradecký kraj, Hradec Králové, Civitas Regina

isss.cz #issscz @issscz triadasro isss-konference

Když se řekne ZONER

ZONER software, a. s., je společnost se sídlem v Brně a pobočkami po celém světě. S více než sto zaměstnanci působí na Slovensku, v Maďarsku, Japonsku a USA. Zabývá se vývojem a distribucí software a je také předním poskytovatelem internetových služeb souvisejících s prezentací na internetu a e-commerce.

Firma má bezmála třicetiletou historii. Vytváří globální produkty pro miliony lidí v oblasti softwaru, bezpečnosti a poskytování internetových služeb. Je rozdělena do čtyř samostatných divizí – fotografický software, internetové služby, on-line bezpečnost a knižní vydavatelství.

ZONER PHOTO STUDIO

Program ZONER Photo Studio X je vlajkovou lodí společnosti ZONER s miliony uživateli po celém světě. Pro zpracování fotografií a fotografickou dokumentaci ho používají jak soukromí fotografové, tak velké firmy a veřejné instituce.

Software nabízí vhodnou alternativu pro širokou skupinu řešení – od bezplatných až po drahé komerční aplikace. Jedná se o nejuniverzálnější program na úpravu fotografií a videí. Umí zpracovat RAWy, podporuje vrstvy, má presety, retušovací nástroje, videostřižnu, katalogizaci, ale i vlastní cloudové řešení a poradí si i s dokumenty PDF.

Kromě zpracování fotografií je v ZONER Photo Studiu X pilotně integrován vícestopý střih videa, což rozšiřuje jeho možnosti při zpracování obrazové dokumentace v situacích, kdy série fotografií nahrazuje videozáznam.

ZPS X je vhodný i ke zpracování fotodokumentace. Nalézají se v něm specifické nezbytné nástroje pro práci ve veřejném sektoru – anonymizace obrazu v souvislosti s GDPR, spolupráce programu s katastrálními mapami nebo databáze RÚIAN pro poloautomatické popisování fotodokumentace metadaty, nejrůznější grafické anotace apod.

WEBHOSTING

ZONER Software, a. s., poskytuje prostřednictvím projektu CZECHIA.COM už víc než 25 let profesionální webhostingové služby desetitisícům zákazníků nejen z České republiky, kterým aktivně spravuje přes 100 tisíc domén. Webhostingové služby nabízí hned v několika variantách – od těch pro operační systémy Windows a Linux, po ty určené konkrétním platformám, jako WordPress, Drupal, Joomla či jiným oblíbeným redakčním systémům.

Nedílnou součástí webhostingových profesionálních služeb jsou i e-mailová řešení s trojí ochranou (antispam, antivir, antiphishing), kde např. u nejoblíbenějšího programu

Linux Plus poskytuje neomezený počet e-mailových schránek a 20 GB prostoru.
Není bez zajímavosti, že ZONER jako jediný v ČR převádí zdarma domény svých zákazníků na zabezpečený HTTPS protokol pomocí exkluzivního SSL certifikátu od největší certifikační autority světa Digicert. Profesionálně, rychle a bezplatně. Pomáhá tím zastavit provoz na zastaralém protokolu HTTP a šířit bezpečnější a šifrovaný HTTPS protokol.

SERVERHOSTING

ZonerCloud.cz společnosti ZONER Software, a. s., nabízí cloudové serverové služby s vysokou dostupností a flexibilitou. Disponuje nejvýkonnějšími servery na trhu, které dokáže zřídit už do 55 vteřin.
Dále se zaměřuje i na pronájem datového prostoru, výpočetního výkonu a individuálních e-mailových služeb.
Jednou z mnoha výhod serverů od ZonerCloud.cz je, že nedochází k žádným latencím a případným výpadkům spojení, protože všechny servery jsou umístěny v ČR. K zajištění absolutního komfortu a bezchybnosti služeb nechal ZONER postavit nové datové centrum v klasifikaci TiER III, které obsahuje nejmodernější technologie od nejspolehlivějších dodavatelů na trhu (DELL a CISCO). Stavba tohoto moderního datacentra vyšla společnost ZONER Software na desítky miliónů Kč.
Společnost ZONER software, a. s., může svědomitě prohlásit, že je skutečný Green energy provider. Na střeše svého sídla vybudovala solární elektrárnu o výkonu 60 kWp, která slouží k napájení vlastního datacentra. Veškerou další potřebnou energii čerpá pouze z obnovitelných zdrojů od předního dodavatele E.ON. ZONER za dlouholeté snažení v oblasti udržitelnosti a ochrany životního prostředí získal jako první v České republice ocenění od uznávané mezinárodní neziskové organizace The Green Web Foundation.

ELEKTRONICKÉ CERTIFIKÁTY A SPRÁVA DOMÉN

Bezpečnostní digitální TLS/SSL certifikáty efektivně chrání před celou řadou kybernetických hrozeb. Obsahují informace o pravosti webu, ověřeném držiteli certifikátu a o datu ověření. Dokazují, že provozovatel není podvodník – díky digitálnímu certifikátu je internetová stránka důvěryhodná, a to jak pro vyhledávače, tak i pro uživatele.
TLS/SSL certifikátem by měl disponovat každý web shromažďující důvěrné údaje. Jen díky němu lze bezpečně zašifrovat názvy, adresy, hesla, čísla účtů, čísla platebních karet a další osobní údaje, aby byly chráněny před hackery a dalšími online podvodníky. U veřejných institucí a úřadů je tedy použití SSL certifikátů pro zabezpečení serverů naprostou nutností.
ZONER software a jeho brand SSLmarket je největším prodejcem TLS/SSL certifikátů v ČR a střední Evropě. Certifikáty poskytuje od roku 2005. Svou prací zajišťuje důvěryhodnost a bezpečnost mnoha významným českým bankám, firmám i úřadům. Svým zákazníkům nabízí rozsáhlé zkušenosti, inovativní technologie, vynikající správu služeb a profesionální zákaznický servis.
Za 14 let spolupráce s předním světovým poskytovatelem TLS/SSL, IoT a dalších PKI řešení, DigiCertem získal SSLmarket už všech 6 prestižních ocenění, která tato společnost uděluje. Kromě ní spolupracuje i s dalšími giganty v oblasti kybernetické bezpečnosti, jako jsou CA QuoVadis či KeyTalk BV.

inPage

Redakční systém inPage od ZONERu je oblíbený nástroj pro tvorbu webových stránek. Ocení ho zejména ti, kteří s vytvářením webové prezentace dosud nemají žádné zkušenosti. ZONER inPage nabízí nejkomfortnější cestu k vytvoření online prezentace, poskytuje jednoduše editovatelné www stránky a webhosting na vlastní doméně (např. CZ, EU, COM, NET, INFO) s elektronickou poštou (10 schránek) a samostatným FTP prostorem.
Pomocí inPage lze vytvořit krásné webové stránky snadno a rychle.

inShop

Součástí společnosti ZONER Software, a. s., je také oddělení e-komerce, provozující nejúspěšnější komerční aplikaci pro provoz internetových obchodů inShop. ZONER inShop je moderní nástroj pro internetový obchod. Nabízí příjemné uživatelské prostředí, pružnost ve funkčnosti i designu a univerzálnost použití. Navíc poskytuje každý nový e-shop formou pronájmu, což zákazníkovi minimalizuje počáteční investice.
Široká škála prodejních a marketingových funkcí dělá ze ZONER inShop ideální řešení pro profesionální e-byznys.

Vojtěch Pospíšil, marketing

Zoner

Zoner Photo Studio

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 6. - 7. 9. 2022

PLATINOVÝ PARTNER: CISCO

GENERÁLNÍ PARTNER: GORDIC

14. ročník výroční konference e-governmentu

6. - 7. 9. 2022

www.egovernment.cz