

JEŠTĚ MÁME ČAS?



JAK UŘÍDIT AI
VE VEŘEJNÉ
SPRÁVĚ

Redakce	OBSAH, TIRÁŽ	2
	ÚVODNÍ SLOVO	4

JEŠTĚ MÁME ČAS	6-7
NOVINKY A PRIORITY DIA V OBLASTI EGOVERNMENTU	8-9
DIGITÁLNÍ STÁT NA PŮL PLYNU	10-12
JE TU ZÁKON, KONEČNĚ	14-15
KAM KRÁČÍME S (V) AI?	18-20
EUDIW	22-23
PODEPISUJTE BUDOUCNOST: DIGITALIZACE VEŘEJNÉ SPRÁVY	24-25
GORDIC: OHLÉDNUTÍ ZA KONFERENCÍ V MIKULOVĚ	26-27
ŘEKNĚTE SBOHEM MANUÁLNÍMU IT! GREENLAKE INTELLIGENCE.	28-29
HYBRIDNÍ CLOUD VE STÁTNÍ SPRÁVĚ: UŽ NEJDE O TO JESTLI, ALE JAK	30-32
POPRVÉ A NAPOSLED	34-35

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

platforma X: @EgovernmentMag

facebook: @EgovernmentMagazin

linkedin: @egovernmentmag

Šéfredaktor: Ing. Michal Jirkovský

Asistentka: Zdeňka Borecká

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

Reprodukce celku ani jeho částí v jakémkoliv provedení není povolena bez výslovného souhlasu Egovernment – info♦com. Neoznačené texty jsou redakčními články.

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**.

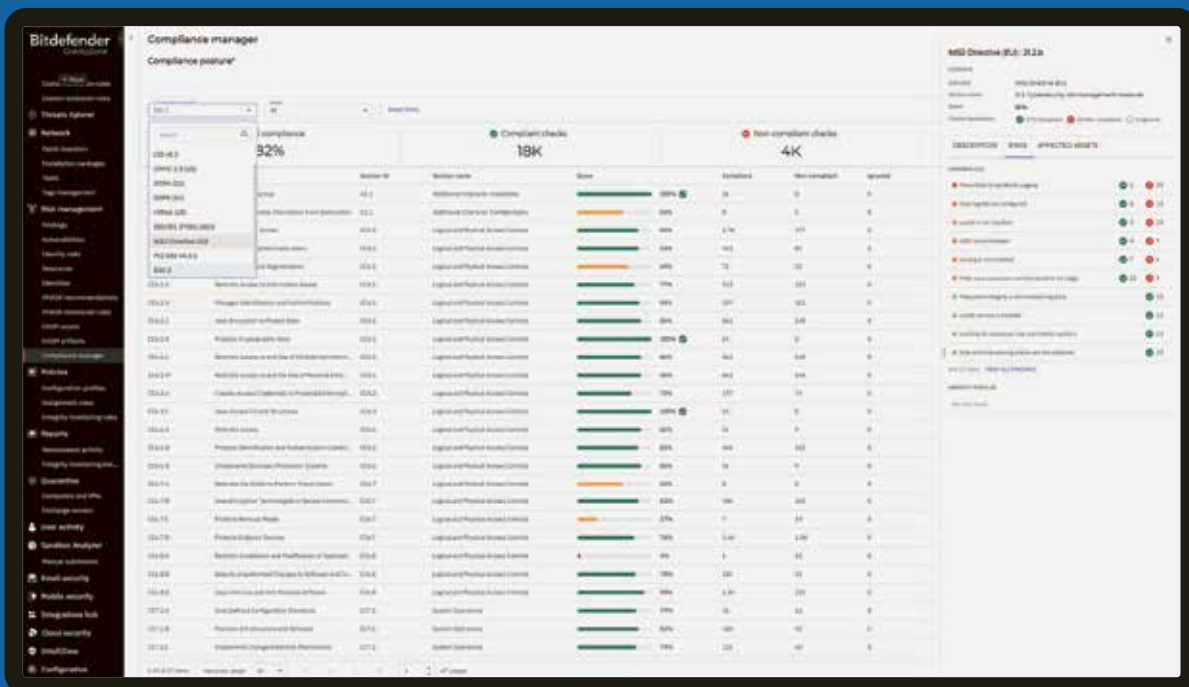
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info♦com s.r.o.**

Global Leader In Cybersecurity



Bud'te připraveni na NIS2 / nový zákon o kybernetické bezpečnosti

Do 31.12.2025 s mimořádnou slevou až 50%



IS4 security
↳ Feel Real Trust

VENDOR
REPRESENTATIVE
COMPANY

Country Partner Bitdefender ČR/SK

email: info@bitdef.cz | tel.: +420 245 501 800

JEŠTĚ MÁME ČAS

Umělá inteligence je všude kolem nás. Nedá se jí uniknout, respektive zprávám o jejím postupu nelze uniknout. Naposledy například informační kanály ohromeně upozorňovaly na skutečnost, že to byla právě AI, která odhadla celkem přesně výsledky voleb. No to je úžasné, zdá se tedy, že nebudeme muset chodit k volbám, protože AI zhodnotí naše nálady a napíše výsledek? Asi ne. Až takto radikálně bychom její pravomoci nechtěli vidět. Tedy většina z nás předpokládám. Je to příliš radikální posun, ale v mnoha jiných oblastech tuto radikalitu nevidíme. Máme pocit, že AI je téměř kouzelná a vyčaruje nám okamžitě ten správný výsledek, ať se jedná o jakoukoliv disciplínu. My lidé jsme už takoví snílci snící o nějakém zázraku. Byli to dot.com firmy, jejichž start provázelo snění a naděje. Pak to prasklo a začalo se znovu trochu reálněji, ale bolelo to. Byly to sociální sítě, o kterých jsme snili, jak nás budou spojoval, jak se budeme všichni kamarádit, sdílet si svoje příběhy, fotografie a názory a jak si vybudujeme hezký svět. A zatím nás to pěkně rozdělilo, někdy až hodně razantně, vyvolává to mezi námi dokonce nenávist a mění se v nástroj šikany. Takže snění a realita jsou skutečně od sebe vzdálené. Patrně i v případě AI jsme nyní ve fázi snění, očekávání, které vždy nemusí být tak docela oprávněné.

Inteligence, která není naše, ale umělá. My ji sice učíme, ale otázka je, zda si za to ručíme. Ona umělá inteligence je samozřejmě prospěšná, ale nebezpečná zároveň. Její rychlost a její výkon jsou takové, že my jím svými mozkovými skutečně nestačíme. A tak se nestačíme divit. Třeba tomu, že to, co nám má pomáhat, nás může šidit. Nebo dokonce jít proti našim příkazům. Ano, jsou to nějaké extrémní případy, ale byly zaznamenány. Neměly bychom je brát na lehkou váhu.

Neměli bychom se ovšem ani přehnaně bát. Mohli bychom tím propásnout šanci, která se nám nyní nabízí. Nejen díky naší šikovnosti, ale do jisté míry i shodou okolností, jsme v tento moment do značné míry připravenější na AI než řada jiných zemí kolem nás. Ještě máme čas se zamyslet. Můžeme, snad, mít vývoj situace ve svých rukách. Naskočit na vlak, který jede správným směrem, podle jízdního řádu, který určujeme my a na kolejích, které jsou pevně ukotveny v zemi.

Michal Jirkovský,
šéfredaktor

Egovernment

elektronizace veřejné správy



Vše o elektronizaci veřejné správy
- srozumitelně a zdarma:
www.egovernment.cz

JEŠTĚ MÁME ČAS

Na konferenci e-government 20:10 na Zámku Mikulov, konané v září, vystoupil prezident Hospodářské komory ČR a ICT Unie Zdeněk Zajíček se zásadním projevem pod názvem „Ještě máme čas“. Chtěl tak upozornit na několik důležitých momentů, kterým bychom v současné době měli věnovat naši pozornost. Aby uvedl své téma, prezentoval citát emeritního profesora Harvardovy univerzity, Edwarda Osborna Wilsona:

**„MÁME PALEOLITICKÉ EMOCE, STŘEDOVĚKÉ INSTITUCE
A TECHNOLOGIE TĚMĚŘ BOŽSKÝCH SCHOPNOSTÍ.“**

Emoce – naše paleolitické emoce – úlek, strach, hněv, radost – se od dob našich praprapra předků příliš nezměnily. Lépe řečeno, vůbec se nezměnily. Stejně jako kdysi, i dnes úlek a strach skokově zvýší adrenalin v našem těle, a to nám velí co nejrychleji a co nejdále utéci. Pouze silou svého rozumu neutíkáme, když nečekaně do kanceláře vstoupí šéf a přistihne nás při lelkování, nebo nás „načapají“ rodiče s mobilem v ruce, byť nám to výslovně zakázali. Tělo by chtělo utéci, je to jeho přirozená reakce. Zůstaneme a sneseme kritiku, či dokonce trest, ale jen proto, že to přemůžeme naším rozumem. Víme, že utéci z kanceláře někam daleko nás nezachrání, ba naopak. Stejně tak zahodit mobil a proklouznout kolem rodičů a prchat nedává žádný smysl. A tak zůstaneme. Ale naše emoce uvnitř s námi cloumají úplně stejně jako před tisíci lety.

Instituce, které máme vybudovány kolem sebe a které tvoří to, čemu říkáme stát a právní řád, jsme budovali dlouho a pečlivě. Vymýšleli jsme si paragrafy, pravidla, omezení a nařízení. Ano, po nějaké době jsme některé z nich aktualizovali a přizpůsobovali, ale pořád stojíme na těch původních, mnohdy poněkud těžkopádných základech, přičemž určité vrstvení dalších norem situaci leckdy dosti zkomplikovalo a učinilo nepřehlednou. Respektive vývoj a modernizace jak oněch institucí, tak zákonů poněkud zaostává, je pomalejší, výrazně pomalejší, než vývoj světa, především pak vývoj technologií. A tak je logické, že náš aparát zdaleka nepostihuje aktuální svět, možná spíše svět našich otců, možná i dědů.

Technologie mají naproti tomu tempo vývoje až brutálně rychlé. Možná překotné. I proto se nám zdá, že jejich schopnosti jsou, nebo mohou být, téměř božské. Je to samozřejmě dáno jejich momentální rychlostí, kapacitou, a tedy výkonem, který se už začíná našemu běžnému chápání vymykát. A tak se stává, že prostě nestíháme. My jsme pozadu! A možná se blížíme bodu, kdy v záchvatu našich emocí se naděje a radostné vítání těchto technologií změní ve strach a obavu a budeme se chtít dát na úprk. Nemáme ale kam. Musíme zůstat a snažit se sladit krok.

MÁME MOŽNOST SE POUČIT

Máme za sebou určité prozření z donedávna vítaných a oslavovaných sociálních sítí. Stejně jako kdysi praskla bublina nadšení a bezmezných očekávání z tzv. dot.com firem, i bezbřehé jásání provázející nástup sociálních sítí vzalo za své. Prostředky, které měly lidi spojovaly a bavily, generují často velké množství negativní energie, strach, paniku a nevraživost. Místo spojování společnost radikalizují a rozdělují, často velice zásadně. Měli bychom si na tomto příkladu uvědomit, že technologie nám mohou pomáhat, a často skutečně hodně, pomáhají. ALE, pokud je neovládáme, neurčujeme pravidla a tak říkajíc nedržíme otěže vývoje pevně v ruce, obrací se proti nám. Je to o to důležitější, že nyní začínáme vítat a vkládat obrovské naděje do něčeho, co nazýváme umělou inteligencí. Do něčeho, co pod naším vedením a naší kontrolou nám může životy skutečně zefektivnit a usnadnit. Ale

přeroste-li nám to přes hlavu, patrně nedokážeme vzdorovat, respektive včas reagovat. Ano, umělá inteligence dělá „pouze“ to, co ji naučíme, ale naučí-li se to, je v tom daleko rychlejší a výkonnější než my. Nebude-li tedy vytvořen rámec pro tyto služby a budou se vyvíjet živelně s nesmyslným očekáváním „světlych zítřků“, můžeme se, až praskne tato bublina, dočkat nemilých překvapení. Ještě je ale čas si uvědomit všechny souvislosti a zvolit správný přístup. Nejde samozřejmě o to být přehnaně opatrný, nebo snad nedělat vůbec nic a nechat si „vlak“ nastupující technologie ujet. Máme například jedinečnou možnost vybudovat v ČR moderní Gigafactory, jako důležitou základnu pro rozvoj AI v rámci Evropy. Na rozdíl od mnoha jiných států, jsme připraveni a schopni v relativně krátké době takové zařízení zbudovat. Bylo by tedy rozumné nenechat si vlak vývoje ujet, ale bylo by žádoucí naskočit na ten, který jede správným směrem a podle našeho jízdního řádu.

PRAVIDLA

Aby se tak stalo, musíme mít především jasnou a srozumitelnou vizi. Musíme tedy vědět, kam a proč směřujeme. Že to není pouze proto, že se jedná nyní o populární téma, ale že je to pro nás skutečně přínosné, a v jakých oblastech je to pro nás přínosem a za jakých okolností. A musíme být schopni tyto skutečnosti vysvětlit i širšímu „publiku“, tedy občanům, proto, aby s takovou vizí byli ztotožnění a byli ochotni ji podporovat, protože tento vývoj bude vyžadovat finanční prostředky, které nebudou nijak malé. Aby se tak stalo, musí v čele vývoje stát schopní, znalí a odvážní politici, kteří si téma vezmou za své, budou je prosazovat, ale zároveň hlídat onen opatrný přístup. A ti by měli upravit zákony, snažit se je přizpůsobit době. Přeskočit z těch mnohdy zastaralých základů do moderní doby. Jedná se především o **Zákon o ISVS**. Ten by měl reagovat na nové možnosti, a to především v oblasti spolupráce veřejného a soukromého sektoru. Měl by mimo jiné nastavit pravidla pro **zadávání veřejných zakázek**, neboť pořízování a objednávání nových technologií už není o nákupu určitého množství konkrétního hardware. Nyní nakupujeme službu a prostor, které nevíme, kdy a v jakém množství je budeme potřebovat, ale tušíme že ten „náraz“ přijde. Podle současného zákona je realizace takového výběrového řízení téměř nemožná. Musíme rovněž být schopni v zákonech podchytit otázku migrace dat – zlatého grálu veřejné správy – a především

pak jejich zabezpečení, tedy kyberbezpečnost, která se vyvíjí rovněž více než dynamicky a není tedy současnými vyhláškami adekvátně podchycena. Je otázka, jestli něco tak rychle a tak rozmanitě bující je vůbec možné popsat nějakou vyhláškou. Ale i na to, že na to nebude vyhláška, by vlastně měla být vyhláška.

DIGITÁLNÍ DVOJČE

Technologický vývoj, tak jak se nyní jeví, je do jisté míry chaos. Veřejná správa, naproti tomu, chaos nepřipouští. Aby tedy byla schopna reagovat na chaotický vývoj nechaotickým popisem, musí si podchycení chaosu nejprve vyzkoušet na „vedlejším hřišti“. Zdeněk Zajíček v rámci svého vystoupení představil tzv. digitální dvojče veřejné správy – prostor kde lze digitálně modelovat vztahy mezi jednotlivými resorty, vztahy mezi jednotlivými informačními systémy a možnost ukazovat co se děje, jak se tyto vazby budou měnit a jaké nároky budou vyplývat z toho, pokud bychom například ubírali agendy určitému resortu, přesouvali je jinam, nebo dokonce určitý resort úplně potlačili. **Digitální modelování** takové změny umožňuje se sledováním efektů i nároků, a to i těch finančních. To je určitá technologická pomoc na cestě dalšího vývoje. Tou druhou je do jisté míry zdravé pročištění právního prostředí, které, vystavěno na zmíněných základech, nás velmi často brzdí. Hospodářská komora má k dispozici konkrétní návrh **antibyrokratického zákona**. A i když zatím nezaznamenala příliš nadšenou odezvu českého politického prostředí, ve spolupráci s kolegy z Dánska a Polska se nyní snaží implementaci tabulky povinností, která z něj vychází, do evropské legislativy.

ZÁVĚR

Jak bylo řečeno, vývoj, který můžeme sledovat, může být pro nás všechny ve svém výsledku velice pozitivní a přínosný a my, jako země, můžeme být jedni z těch, kteří výrazně ovlivňují jeho další směřování, a to nejen v rámci našich hranic. Ale také se může stát, že nám „uteče“, předběhne nás a my se budeme klopýtat snažit o nemožné, totiž srovnat s ním krok. Jde tedy „jen“ o to naskočit na ten správný vlak. Ještě je čas se rozhodnout, ještě je čas ujasnit si, co a jak chceme, čeho jsme schopni a kam až technologie chceme a může pustit.

NOVINKY A PRIORITY DIA v oblasti eGovernmentu

Ředitel Digitální informační agentury Martin Mesršmíd je, z titulu své funkce, již tradičním účastníkem a zároveň vystupujícím na konferenci v Mikulově. Letos hovořil o projektech DIA, které jsou dokončeny, či těsně před dokončením, a věnoval se i určitému výhledu do budoucna. Veškeré projekty či produkty jsou v rámci DIA rozděleny do čtyř pilířů – pro úřady, pro občany, legislativní metodická pomoc a přímá podpora úřadům. Postupně ve svém vystoupení prošel všechny čtyři zmíněné oblasti.



SMUTNÝ POHLED ROZJASNÍ FORMULÁŘE

Naplňování Zákona o právu na digitální službu je do jisté míry smutným pohledem na to, jaký je stav digitalizace. Došlo sice k prodloužení účinnosti části tohoto zákona a vláda svým usnesením stanovila nepřiměřenou zátěž, respektive některé služby se přesunuly do nepřiměřené zátěže. To je jistě možné vnímat pozitivně. Problematická je však skutečnost, že za celou dobu, co se naplňoval zákon o právu na digitální službu, bylo zdigitalizováno pouze 20 % služeb.

Při komunikaci s jednotlivými resorty, kdy se DIA snažila identifikovat, které služby jsou zdigitalizovány a u kterých to je možné, došlo i na diskuzi o těch agendách, které budou zdigitalizovány teprve v budoucnu. Debata se samozřejmě týkala především toho, kdy jsou resorty schopny spustit elektronická podání, respektive příslušné formuláře, a ukázalo se jako žádoucí, aby existoval jednoduchý nástroj, kterým je možné elektronický formulář vytvořit rychle a snadno. Spousta podání má totiž velice jednoduchý charakter, pouze o několika málo položkách. Proto DIA vyvinula tzv. zjednodušené formuláře, nástroj, kterým je možné během maximálně 30 minut vytvořit formulář, který je schopen přijímat data od uživatele a předvyplňovat nezbytné položky. Martin Mesršmíd upozornil, že díky registru zastupování je možné učinit toto podání i v zastoupení. Jedná se tedy o nástroj, který je **schopen velice snadno naplnit zákon o právu na digitální službu**.

Samotný proces spočívá ve vyplnění jednotlivých požadovaných položek formuláře v RPP. Formulář je následně vygenerován a během několika minut je k dispozici jeho URL, na kterou je možné odkazovat, nebo ji přímo vložit do vlastního portálu. Samozřejmě je DIA v případě potřeby nápomocna při osvojování tohoto prostředku.



DIGITALIZACE PROCESŮ DIA

Proces schvalování projektů OHA měl doposud jednu zásadní chybu, nebyl kompletně digitalizován. Princip schvalování spočíval ve vyplnění off-line formuláře, který byl zasílán do datové schránky DIA a následně posuzován odborníky OHA. V současné době je spouštěn informační systém dlouhodobého řízení, který umožňuje vyplnění formuláře s on-line asistencí a zároveň dojde k určitému propojení žadatele se schvalovatelem. Žadatel může tedy sledovat proces schvalování, případně doplňovat do formuláře další informace. Celý průběh je tak transparentnější a rychlejší. Dá se říci, že se jedná o průlomový projekt i proto, že byl realizován jako zakázkový software od CENDIS, nicméně se zapojením odborníků OHA, kteří jej mohou dále doplňovat a rozvíjet.

Druhý aktuálním systémem, který nyní DIA buduje a který by měl v plném rozsahu fungovat začátkem příštího roku, je **informační systém Cloud Computingu**. Samotný Cloud Computing je pro další rozvoj e-governmentu naprosto zásadní a DIA předpokládá, že Česká republika by se měla při dalším rozvoji informačních systémů ubírat právě touto cestou. Nyní budovaný informační systém by měl umožnit spravovat zápisy do katalogu Cloud Computingu. Bude se jednat rovněž o zcela nový katalog. DIA by v tomto smyslu měla být schopna fungovat v roli centrálního zadavatele, respektive být nápomocna jednotlivým úřadům vysoutěžit jakoukoliv službu uvedenou v katalogu. Pro centrální služby jsou již k dispozici vzorové smlouvy, a tak Martin Mesršmíd v Mikulově vyzval všechny k vyzkoušení tohoto nástroje.

Informační systém modelování dat je další systém, na kterém DIA aktuálně pracuje. Datové modely nejsou ničím,

s čím by se veřejná správa tradičně setkávala, přitom to může být základ dalšího rozvoje e-governmentu. Díky datovému modelování budeme schopni analyzovat situace a přesněji se rozhodovat o dalším postupu, ovšem, a to je důležité, pouze na základě dostatečného množství relevantních dat. Informační systém je navržen tak, že vede datového analytika celým procesem od analýzy zákona až po vytvoření datových slovníků a k popisu těchto dat. Jedná se o praktické využití AI, která je schopna analyzovat zákon ze kterého se vychází, navrhnout jednotlivé pojmy v datovém slovníku, navrhnout atributy těchto pojmů a celý tento slovník připravit k posouzení. Systém by měl být tedy nápomocen jak v naplňování zákonných povinností, tak v lepším sdílení a využití dat, která máme k dispozici.



PRODUKTY PRO OBČANY

Informační systém datových schránek – mělo by dojít k publikování několika zásadních vylepšení, která byla identifikována jako žádoucí na základě průzkumu mezi uživateli (byla publikována v průběhu září). Jedná se především o přepínání mezi datovými schránkami, které je nyní daleko jednodušší, respektive s menším počtem kroků. Dalším zlepšením by mělo být zvýšení doby uložení datových zpráv, pohodlné náhledy příloh, tak aby nebylo nutné ji vždy stahovat, a přehledné e-mailové notifikace.

Další změna se týká **registru zastupování**, který byl spuštěn v loňském roce. Byl zpřístupněn portál registru zastupování, od července je pak k dispozici možnost podání žádosti o zápis oprávnění na kontaktních místech veřejné správy (CZECH Pointech). Zároveň probíhá další analýza jednotlivých ohlašovatelů agend a tvorba šablon, které odpovídají jejich agendám. Vše směřuje k tomu, aby občan, který se přihlásí do Portálu, přehledně viděl, koho může zastupovat. Zároveň byl registr zastupování implementován i ve zmiňovaných zjednodušených formuláři. Do konce roku by pak mělo v rámci portálu být možné, aby občané z vytvořených šablon mohli založit jakékoliv zmocnění k zastupování.



EVROPSKÁ PĚNĚŽENKA DIGITÁLNÍ IDENTITY

Jedná se o jeden z největších současných projektů, o nástroj, který by měl zásadně změnit způsob nakládání s digitální identitou, propojit předávání informací mezi

státem a soukromým sektorem a také umožnit soukromému sektoru nové obchodní modely založené na využití systémů vytvářejících důvěru. Aktuálně je v přípravě státní část evropské digitální peněženky, která bude umožňovat prokazování elektronické identity občana a zároveň osvědčení o konkrétních attributech (o dosaženém vzdělání, bezdlužnosti a dalších, které jsou obsaženy v informačních systémech veřejné správy). Digitální informační agentura ve spolupráci s jednotlivými resorty vytipovala řadu konkrétních příkladů použití – od běžné identifikace až po využití například ve zdravotnictví pro uchovávání dat o lékařských předpisech či zdravotnické dokumentace atp. Nyní rovněž probíhá vypořádávání připomínek, které DIA obdržela v rámci meziresortního připomínkového řízení k návrhu adaptační legislativy. Na úrovni Evropské komise se pak pracuje na specifikaci některých implementačních aktů. Je to poněkud náročné, když pravidla provozu vznikají takřkajíc za běhu, ale vše směřuje k tomu, abychom skutečně mohli koncem roku 2026 disponovat Evropskou peněženkou digitální identity. (Více jsme se tomuto tématu věnovali v rámci diskuze, která je popsána na stránce 22.)



VÝHLED DO BUDOUČNA

Pro další vývoj elektronizace veřejné správy by bylo patrně vhodné trochu změnit uvažování o tom, jak budujeme naše informační systémy. Především bychom měli daleko více využívat sdílených služeb i sdílené infrastruktury. Výsledkem by měla být situace, kdy se úřady věnují především své věcné rovině, nikoli otázkám licencí, vybavení atp. Takový přístup samozřejmě otevírá prostor pro využití zmiňovaných Cloudových služeb. Zároveň bychom se měli zaměřit na transparentnost a měření dopadů – efektivitu a fiskální udržitelnost. Moderní e-government by tedy měl nabízet digitální služby pro občany, které jsou jim skutečně přizpůsobené a užitečné. V další transformaci veřejné správy bude samozřejmě velice podstatná role AI. I proto se DIA ve spolupráci s ICT Uníí rozhodla vytvářet seznam příkladů využití, respektive konkrétních implementací ve veřejné správě, jako vodítko pro ostatní při jejich rozhodování. V této souvislosti zmínil Martin Mesřmíd tzv. Digitální dvojče, o kterém více hovořil ve svém vystoupení Zdeněk Zajíček. Martin Mesřmíd to považuje za velice důležitý koncept, který může simulovat a predikovat změny a jejich dopady s dlouhým výhledem dopředu, a tedy výrazně zefektivnit e-government.

DIGITÁLNÍ STÁT NA PŮL PLYNU

Česko má na to být evropským lídrem digitalizace, jen tento potenciál zatím neumí plně využít

Česko má na to mít jedny z nejlepších digitálních služeb na světě. Ale zároveň tento potenciál využívá minimálně a téma digitalizace je spíš popelkou na žebříčku politických priorit. Proč to tak je a co se s tím dá dělat, zmapovaly v rámci projektu Služby.Digital dvě neziskové organizace, které kombinují značné know-how v oblasti digitalizace a společenského výzkumu: Česko.Digital a analytický ústav STEM.

„Chtěli jsme se na digitalizaci státu podívat z perspektivy všech, kteří s ní nějak přicházejí do kontaktu,“ přibližuje výzkumnou část projektu Jiří Táborský, který měl projekt ve STEM na starosti. Výzkumná část projektu zahrnovala dotazníkové šetření na reprezentativním vzorku dvou tisíc občanů ČR, osm fokusních skupin či dotazníkové šetření mezi 300 firem. Dotazování obsahovalo i více než 70 hodin hloubkových rozhovorů s 50 respondenty z řad politiků, kteří se zabývají tématem digitalizace, úředníků z centrální státní správy, zástupců hlavních dodavatelských firem a úředníků ze samospráv na úrovni obcí a krajů.

„Cílem projektu Služby.Digital je pomoci vzniku špičkových digitálních služeb státu. Takové služby šetří obča-

nům i firmám čas a peníze a jsou přístupné pro každého. Jsou také efektivní z pohledu provozovatele a splňují ty nejnáročnější požadavky v oblastech kybernetické bezpečnosti nebo UX designu,“ přibližuje cíle projektu Blanka Šoulavá, která projekt vede v organizaci Česko.Digital a která je zároveň spoluautorkou doporučení pro příští vládu.

Ve výsledcích výzkumu na první pohled zaujme, že přes 90 % veřejnosti považuje digitální služby za své právo. Zároveň je však třeba dodat, že stejný podíl populace požaduje zachování i analogové cesty. U firem pak rozhodně převažuje preference digitálu. Nicméně ačkoliv lidé považují digitální služby za samozřejmost, spokojenost s nimi vyjadřuje jen cca 40 % z nich.

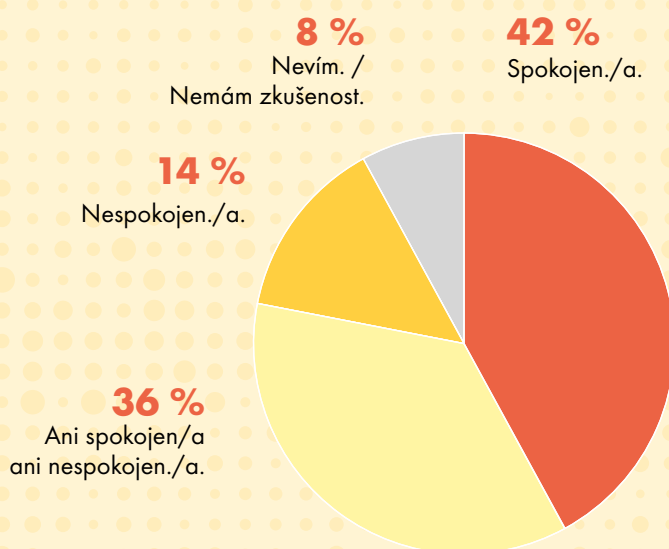
Jen 4 z 10 občanů jsou spokojeni se stavem digitalizace.

Otázka:

„Při uvážení všeho, na co jsme se dotazovali, jak jste celkově spokojeni/a se současným stavem digitalizace veřejné správy v České republice (např. on-line formuláře, komunikace s úřady přes internet, Portál občana apod.)?“

Zdroj: Výzkum STEM pro Česko.Digital, květen 2025

Odpovědi:



Výzkum se také zaměřil na vlastnosti, které podle Informační koncepce České republiky mají digitální služby mít. U každé z vlastností se měřila důležitost z pohledu uživatele a pak to, nakolik státní služby tyto vlastnosti reálně naplňují. Jednoznačným vítězem je bezpečnost,

která je pro lidi zcela stěžejní a která se projevuje například tím, že naprostá většina lidí preferuje, aby jejich data spravoval stát, případně soukromé firmy, ale pod silnou regulací státu.

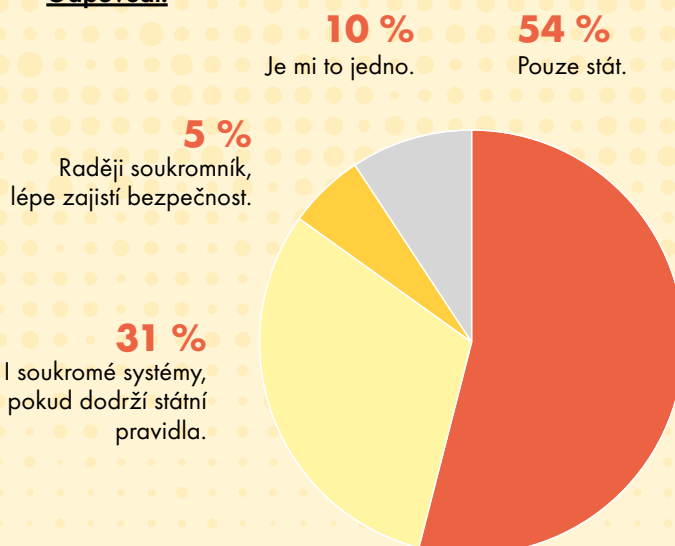
Mírná většina si myslí, že by k datům neměl mít přístup nikdo jiný než stát.

Otázka:

„Ve státních digitálních systémech je dnes řada citlivých dat, například z daňových přiznání, zdravotní data apod. Která z následujících možností nejlépe vystihuje Váš názor na to, kdo by měl tato data spravovat?“

Zdroj: Výzkum STEM pro Česko.Digital, květen 2025

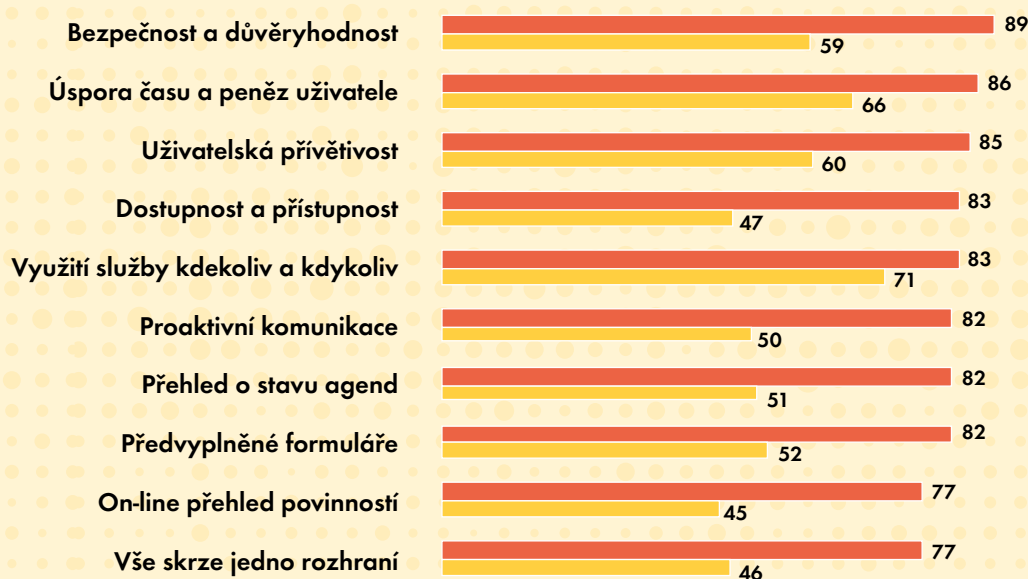
Odpovědi:



Nicméně všechny vlastnosti, které vyplývají z koncepce, se jeví jako klíčové. Vidíme však velký rozdíl mezi tím, jak lidé vnímají důležitost těchto vlastností a jak hodnotí jejich reálný stav. Největší rozdíl 36 procentních bodů

je v oblasti dostupnosti a přístupnosti, to znamená možnost využít službu, i pokud máte nějakou bariéru, například zdravotní či jazykovou.

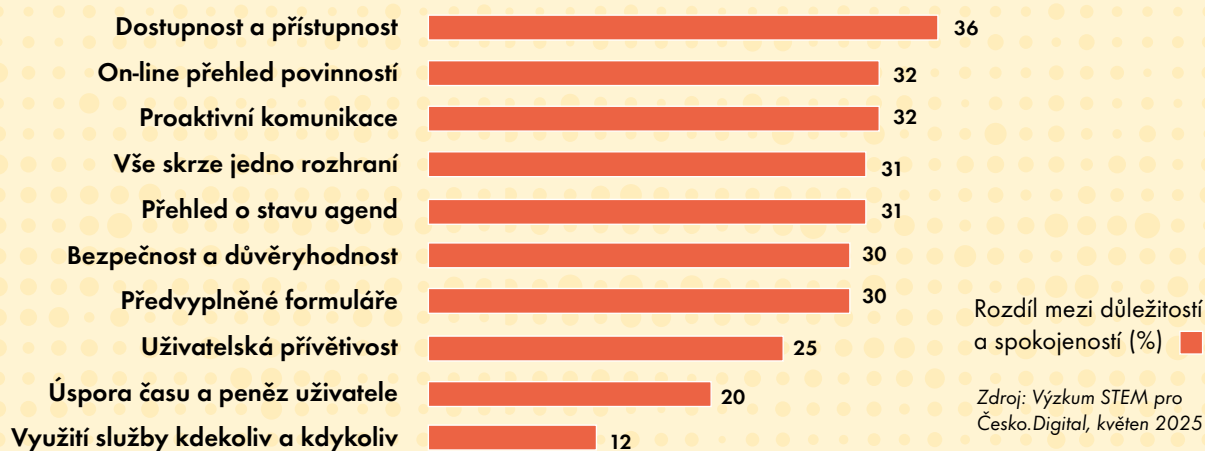
Co občané od služeb očekávají a jak jsou spokojeni?



Důležitost % ■ Spokojenost % ■

Zdroj: Výzkum STEM pro Česko.Digital, květen 2025

Rozdíl mezi očekáváním a realitou



V oblasti hloubkových rozhovorů s experty z různých sfér se výzkum zaměřoval na příležitosti, tj. na to, co je v Česku dobré, a také na bariéry, proč se nám rychlejší postup nedaří. „V oblasti úspěšných příkladů většina respondentů celkem spontánně zmiňovala základní registry. Ne jako systém (ten je technologicky už více méně za zenitem), ale spíše celkovou koncepci a legislativní ukotvení. Dále v Česku máme značné množství úřadů a projektů, které mohou sloužit jako inspirace pro ostatní. Velmi dobrého hodnocení se dostalo Portálu dopravy nebo celkovému digitalizačnímu úsilí Ministerstva práce a sociálních věcí. Podobně je dobře hodnocen Český úřad zeměměřický a katastrální,“ popisuje Táborský s tím, že na tom lze dobře ilustrovat dva klíčové faktory, bez kterých se digitalizace nepohne dál: politická podpora a dlouhodobá strategie a kontinuita. „Pokud nebude mít digitalizace faktickou podporu napříč vládou a nebude jasná centrální autorita, která bude určovat a držet směr digitalizace, tak je pokrok prakticky nemožný,“ uvádí Šoulavá s tím, že právě nastavení tohoto systému patří ke klíčovým změnám, bez nichž se nepohneme kupředu a také nepřekojíme často zmiňovaný problém resortismu, tj. fixace politiků a úředníků na dění ve vlastním resortu a neochotu spolupráce napříč státními institucemi.

Jako další zcela esenciální oblast se jeví odborné kapacity. Stát dlouhodobě není schopen nastavit konkurenceschopný systém odměňování. A netýká se to jen programátorů. Stejný problém je u procesních analytiků, architektů a dalších expertů. „Už nevidíme vendor lock-in způsobený nevýhodnou smlouvou, ale často vidíme právě ten znalostní, kdy stát nemá know-how nebo kapacity pro správu velkých IT projektů. Řešením není nic jiného než zlepšit konkurence-

schopnost státu na trhu práce oproti soukromému sektoru,“ říká Šoulavá.

Další neméně důležitou oblastí je management kvality. Šetření ukázalo, jak málo toho stát ví o efektivitě služeb, které nabízí. Chybí průběžné měření spokojenosti uživatelů, chybí vyhodnocování efektivit investic do IT optikou úspory nákladů a chybí také zpětná vazba od uživatelů systému z řad úředníků. „Platí, že co neměříme, to neřídíme. A náš stát toho měří málo, a pokud už nějaká data má, tak s nimi obvykle nepracuje, a to nejen v oblasti digitalizace, ale obecně při nastavování veřejných politik,“ poznamenává Táborský.

Poslední ze zásadních oblastí je legislativa a obecně tvorba procesů. V řadě oblastí legislativa komplikuje automatizaci, protože trvá na rigidních procesech s lidskou účastí. Další problém je, že v řadě resortů nejsou IT odborníci přítomní tvorbě legislativy a obecně nastavování procesů.

„Celkový pohled, který nám projekt poskytl, je v zásadě optimistický. Sice přetrvává několik hlavních bariér, jako je nedostatek politické podpory, problémy v oblasti fungování státní správy, resortismus, nedostatek lidí a další, ale je zřejmé, že i navzdory těmto potížím se podařilo vybudovat solidní základy a řadu špičkových služeb. Skepticismus většiny lidí uvnitř systému je dán spíše tím, že vidí, na jakém potenciálu Česko sedí, ale zároveň vidí, jak je tento potenciál nevyužíván,“ uzavírá Táborský.

Využití tohoto potenciálu naplno je právě cílem projektu Služby.Digital a další aktivity organizace Česko.Digital se budou věnovat zejména prosazování jednotlivých doporučení ve spolupráci s partnery a členy komunity Hybatelů digitálního Česka. Všechna podrobná zjištění vč. dat a doporučení najdete na webové stránce www.sluzby.digital

Česko.Digital, analytický ústav STEM



Požadavky nové regulace NIS2 nabývají účinnosti 1. 11. 2025.

Hledáte řešení?

Přinášíme vám pomoc a řešení pro splnění zákonných požadavků NIS / KYBE: limitovanou nabídku aplikace ICZ Risk*Guide. Modulární nástroj pro řízení a analýzu rizik kybernetické bezpečnosti, umožňuje efektivní identifikaci, hodnocení a mitigaci kybernetických rizik a poskytuje podklady pro audit z NÚKIB.



Využijte naši mimořádnou nabídku. Zvýhodněná cena je limitovaná termínem objednání do 30. 11. 2025.
Podrobnosti najdete na webu:



 **ICZ Risk*Guide**

*S kybernetickou bezpečností
máme zkušenosti, obraťte se na nás.*

ICZ

www.iczgroup.com

JE TU ZÁKON, KONEČNĚ

Do jisté míry jsme se docela dlouho těšili, a možná i obávali, existence nového Zákona o kyberbezpečnosti. Nyní máme již jasno, zákon je zde a 1.11. 2025 na nás dopadne celou svou vahou. Vyplyvá z něj řada povinností jak pro velké množství úřadů, které se doposud zákonem řídit nemuseli, tak pro samotný regulační úřad, kterému právě díky velkému množství nových povinných subjektů skutečně skokově vzroste práce. I proto jsme se, nejen o Zákonu, bavili s ředitelem NÚKIB Lukášem Kintrem.

Lukáš Kintr zdůraznil, že je skutečně rád, že po deseti letech máme v ČR doopravdy soudobý kybernetický standard, protože za těch deset let od vzniku poslední normy došlo k výraznému posunu a stávající zákon skutečně přestával vyhovovat, neboť nedržel krok s technologiemi, a tedy neodpovídal současné době.

Nový zákon bude účinný od 1. listopadu 2025, ale před NÚKIBem je do té doby ještě dost práce na prováděcích předpisech, které by měly být k tomuto datu připraveny. Samozřejmě, jak bylo již řečeno, znamená to celé spoustu práce navíc pro samotný úřad. Ale je to práce, o které NÚKIB dlouho dopředu věděl, počítal s ní a je zřejmé, že se musí adaptovat na větší počet institucí, jimž musí být partnerem. Mimo jiné to dává i prostor k tomu zvažovat, kde a jak využít v tomto směru nástroje AI. Je jisté, že některé dotazy bude nutné agregovat tak, aby je NÚKIB zvládal odbavit včas v předpokládaném množství, ale to by neměl být problém. U samotných subjektů Lukáš Kintr rovněž nepředpokládá problémy, neboť, jak věří, jedná se o firmy a instituce, které se kyberbezpečnosti věnovaly už před dopadem samotného zákona, a to čistě z pudu sebezáchovy.

Tento Zákon míří především na střední a velké podniky, malých se dotýká jen v některých specifických případech. Stejně tak v případě veřejné správy je cíleno především na obce s rozšířenou působností, tedy subjekty, které mají pro celkový chod nějaký zásadnější význam. A v těchto případech považujeme za zcela samozřejmé, že se zabývají otázkami kyberbezpečnosti, protože se jedná o hrozby, které mohou být například pro střední firmy ve svém důsledku až likvidační, když taková napadená firma stojí před dilematem, zda s vyděračem vyjednávat, zaplatit či nezaplatit. Plnění požadavků zákona je tedy v tomto

směru skutečně něco, co je jejich vlastním zabezpečením a samozřejmostí.

K samotnému, poněkud zdoluhavému, procesu přijímání nového zákona Lukáš Kintr uvedl, že je asi velice těžké připravovat normu, která má takto široký regulační dopad. Čím více subjektů pod něj má spadat, tím více se objevuje komentářů a podnětů, a to často i protichůdných. Probrat se jimi je tedy skutečně minimálně časově velice náročné. Je tedy těžké odhadnout, co bylo možné urychlit. Berme to spíše tak, že žijeme v nedokonalém světě a cokoliv nového připravujeme, má nějaké porodní bolesti a je provázeno komplikacemi. Ale teď to vypadá, že se podařilo připravit komplexní zákon, který kvalitně postihuje současnou situaci a o kterém je možné předpokládat, že s námi stráví, respektive my se jím budeme řídit, dalších deset let.

Samozřejmě implementace evropské normy (NIS2) do českého prostředí není úplně jednoduchá. NÚKIB se soustředil především na to, aby se podařilo text co nejvíce přizpůsobit české realitě. Je jasné, že evropské znění míří na celou Evropu obecně a je tedy nutné jej nějak konkrétně zasadit do racionálního rámce konkrétního regionu tak, aby skutečně fungoval. Největším zádrhelem debat ve Sněmovně byla bezpochyby bezpečnost dodavatelského řetězce. To přímo nesouvisí s transpozicí NIS2, ale jedná se o reakci na zadání ještě předchozí vlády, tedy reakci na určité národní požadavky národní bezpečnosti. Celý mechanismus je nyní navržen tak, že NÚKIB bude ve spolupráci s celou řadou zapojených institucí vyhodnocovat dodavatelské řetězce u cca 150 subjektů poskytujících strategicky významnou službu. Na základě těchto vyhodnocení bude pak vládě navrhopvat konkrétní opatření.



NEJEN ZÁKON, ALE I INCIDENTY

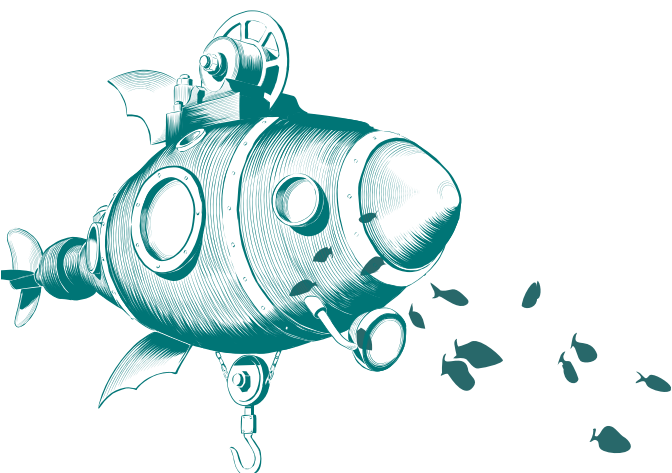
V rámci ČR došlo v nedávném období k několika bezpečnostním incidentům, dokonce i v rámci MZV. Právě tento případ ukázal, že schopnost státu koordinovaně postupovat v oblasti kyberbezpečnosti je velice vysoká, a to i v porovnání se zahraničím. Je samozřejmé, že úplně ideální by bylo, kdyby k takovým situacím nedocházelo, ale pokud k nim dochází, je potěšující, že jsme schopni reagovat, a to na světové úrovni.

Samotná oblast kyberbezpečnosti se podle Lukáše Kintra, i přes nástup umělé inteligence, bez zásahu lidského faktoru ještě zcela neobejde. Ale samozřejmě je nutné všechny tyto prostředky akceptovat a využívat k obraně, protože je zřejmé, že jsou používány na té druhé straně, ze strany útočníků. A ta „soutěž“ s útočníkem nikdy nekončí a je vždy jen otázkou, kdo je schopen reagovat rychleji a efektivněji a tomu samozřejmě nástroje AI mohou výrazně napomoci.

NÁRODNÍ STRATEGIE

Národní strategie kyberbezpečnosti navazuje na předchozí období, pracuje s několika premisami a je navázána na mezinárodní spolupráci. Ve svém důsledku se dotýká odolnosti naší společnosti. Aby však dávala jakákoliv strategie smysl, musí zapadat do právního rámce a být uplatnitelná v praxi, tedy reagovat na skutečnou situaci. Vedle umělé inteligence je tématem současnosti i kvantová hrozba. Musíme jako stát přecházet na odolné šifrování, protože jenom tak si zajistíme odolnost našich informací, našich dat i do budoucna. Zároveň je třeba reflektovat i určitý nedostatek personálních kapacit, což je problém pro státní i soukromý sektor. Musí zde být dostatečná motivace, a to nejen finanční, která bude skutečně atraktivní pro zajištění expertů do této oblasti. A kromě samotného hledání je samozřejmě dobré vytvořit i podmínky pro jejich výchovu – v rámci studia.

Samotná strategie má pětiletý horizont, ze zákona je povinnost ji minimálně jednou za pět let aktualizovat, což je proces, kterým jsme právě prošli. Nyní tedy pokrýváme období 2026–2030 a někdy v průběhu tohoto období, kdy budeme cítit, že přestává vyhovovat či stačit, bude nutná její další aktualizace.



SIEM Essential

Řešení kybernetické bezpečnosti pro malé a střední podniky s integrovanou možností automatizace (SOAR)

Pro odhalení stále účinnějších a sofistikovanějších kybernetických útoků již nestačí používat tradiční nástroje, jako jsou například IPS (Intrusion Prevention System) nebo antivirus. Nutností je nasazení pokročilejší technologie založené na korelaci velkých dat, umělé inteligenci a strojovém učení.

Účinné detekce lze docílit pouze tehdy, pokud sbíráte a vyhodnocujete logy z nejrůznějších zařízení v reálném čase. Ty pak pomocí analýzy a korelace vyhodnocujete tak, aby odpovědní pracovníci za bezpečnost dostávali relevantní informace událostech a anomáliích v rámci infrastruktury vaší firmy.

Pokud patříte mezi malé nebo středně velké společnosti, které nepotřebují komplikované řešení s rozsáhlou implementací, a neznáte dopředu rozsah a objem dat, která je potřeba pro zajištění bezpečnostního dohledu sbírat, máme pro vás ideální řešení. Je jím SIEM Essential postavený na technologii SPLUNK. Díky předdefinovaným scénářům vytvořeným na základě rámce MITRE ATT&CK a široké škále integrací na podporované aplikace lze nasazení do prostředí zákazníka provést v řádu dní.

Výhody řešení SIEM Essential od ALEFu:

- instalace do 14 dnů
- pevná cena za licenci na zaměstnance
- předpřipravené detekční scénáře odpovídající prostředí daného zákazníka
- díky vestavěné integraci se Splunk SOAR (Security Orchestration, Automation, and Response) možnost efektivního zapojení automatizace
- integrace na nejčastěji používané aplikace z enterprise prostředí
- nízké procento false positive událostí
- efektivní detekce kybernetických hrozeb
- naplnění legislativních požadavků Zákona o kybernetické bezpečnosti
- snadná migrace do robustního plnohodnotného SIEMu
- široké možnosti využití Splunku i v jiných oblastech (IT, business, marketing)
- Možnost implementace zákaznických aplikací
- Možnost rozšíření z více než 1600 korelačních pravidel vyvíjených vendorem

Pro koho je SIEM Essential primárně určen?

- pro organizace s počtem zaměstnanců v rozsahu od 100 do 700 zaměstnanců
- pro organizace bez zkušeností s logováním a vyhodnocováním bezpečnostních incidentů a událostí
- pro organizace bez SOC týmu
- pro organizace, které potřebují získat komplexní pohled na bezpečnostní situaci, dodržovat předpisy a standardy a zlepšit obranyschopnost proti kybernetickým hrozbám

PROČ ZVOLIT ŘEŠENÍ SIEM ESSENTIAL OD ALEFu?

Managed služba (Software as a service)

- Dedikovaný tým bezpečnostních specialistů zajišťující provoz a údržbu systému
- Pravidelná aktualizace vyhodnocovacích scénářů dle aktuálních hrozeb
- Pravidelná aktualizace systému a profylaxe
- Efektivní řešení s nízkými náklady na implementaci

MOŽNOSTI INSTALACE

1



ON-PREMISE

- › HW zákazníka
- › Dodávka nového HW (Možnosti financování přes ALEF Financial Services)
- › Virtuální prostředí zákazníka (VMware, Hyper-V, ...)

2

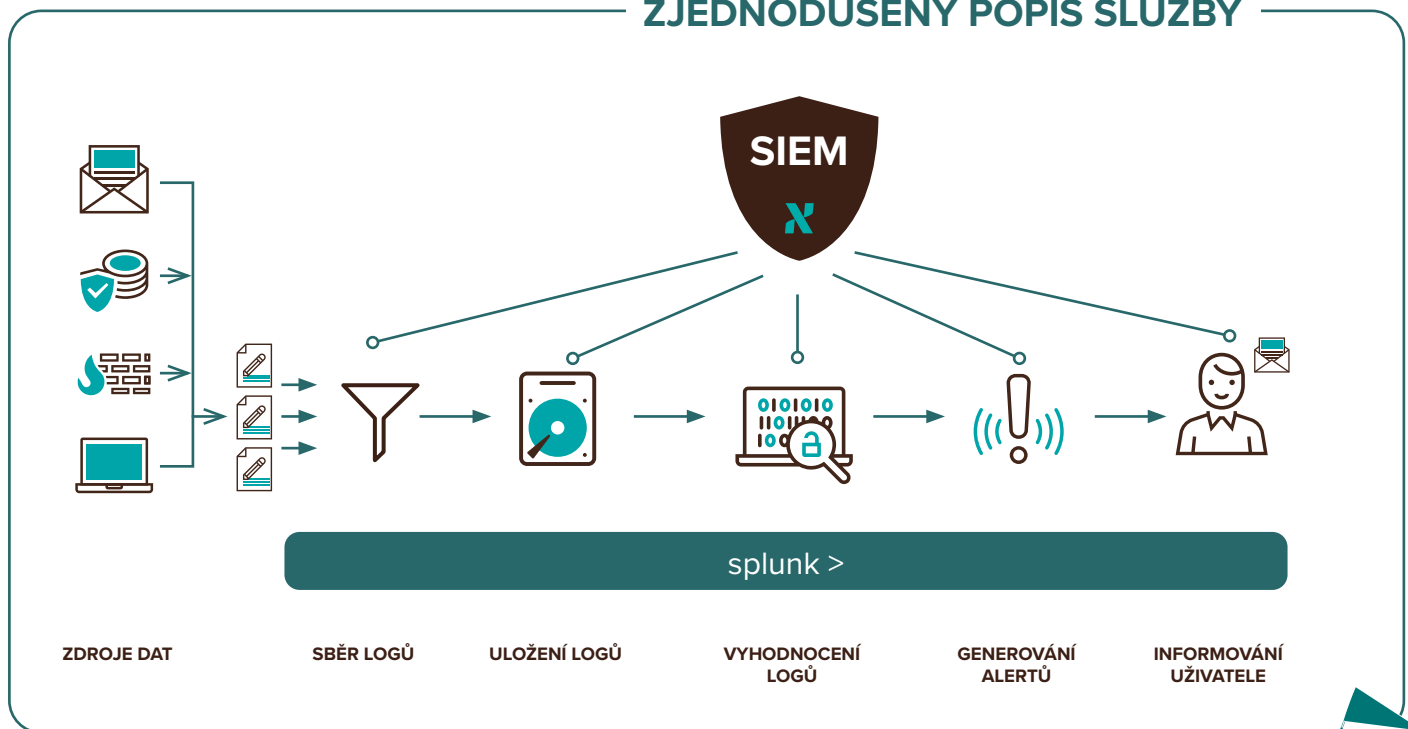


CLOUD

- › Cloud zákazníka
- › Veřejný/privátní cloud (AWS, MS Azure, ...)



ZJEDNODUŠENÝ POPIS SLUŽBY



Obsah dodávky:

- Pronájem licence SPLUNK Enterprise + Cribl
- Pronájem licence Splunk SOAR (Security Orchestration, Automation, and Response) - volitelné
- Detailní popis nastavení zdroje dat
- Detailní popis detekčních scénářů
- Testovací scénáře
- Obecně platné playbooks pro vybrané detekční scénáře
- Připravené dashboardy a reporty
- Základní zaškolení
- 2 hodiny konzultace měsíčně v ceně služby

Průběh implementace

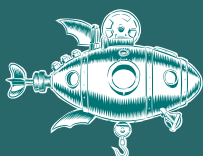
1. Vytvoření High-level design/Low-level design pro implementaci SIEM Essential
2. Instalace systému v prostředí zákazníka/cloudu
3. Nastavení zdroje dat ze strany zákazníka dle dodaného návodu
4. Kontrola vstupů a vyhodnocení instalace
5. Validací testy
6. Zaškolení obsluhy
7. Předání do provozu

DOPLŇKOVÉ SLUŽBY

- 1 Bezpečnostní konzultace nad novými systémy a hrozbami
- 2 Bezpečnostní analýza
- 3 Konzultace k vyhodnocení vzniklých bezpečnostních incidentů
- 4 Pasivní asset management
- 5 Pasivní vulnerability management

Další doporučená témata a oblasti z kybernetické bezpečnosti:

- Audit kybernetické bezpečnosti
- Implementace ISO 27001
- Bezpečnostní testování a Phishingové kampaně
- Security Awareness Training (školení bezpečnostního povědomí)
- Firewall + EDR (Endpoint Detection & Response) + MFA (Multifaktorová autentizace)



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691 /42, 186 00
Praha 8, Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

Kontakt:

Jan Hrubý | Business Unit Manager for Splunk
Phone: +420 777 101 037 | jan.hruby@alef.com



Kam kráčíme s (v) AI?

Navázali jsme na vstup vládního zmocněnce pro AI Jana Kavalírka, který měl v rámci konference v Mikulově a povídali si s ním o aktuální situaci kolem umělé inteligence. Samozřejmě nás zajímalo především to, jak vypadá současný stav výběru na realizaci Gigafactory?

V současnosti se intenzivně věnujeme přípravě naší národní přihlášky. Zřídili jsme si koordinační radu pro AIGF, která se pravidelně schází a koordinuje přípravu napříč státní správou, výzkumnou sférou i soukromým sektorem. Nyní připravujeme první materiál pro vládu, jehož cílem je schválit mandát pro přihlášku České republiky, deklarovat státní podporu tohoto strategického projektu a současně dát úkol našemu ministerstvu rozpracovat projekt a navrhnout jeho financování. Strategicky pak zvažujeme i sektorovou specializaci AI Gigafactory – například směrem k obraně, kybernetické bezpečnosti či využití vesmírných dat.

Kromě toho intenzivně jednáme jak doma – zejména o zajištění národního financování a České radiokomunikaci o privátním financování – tak i na evropské úrovni s jednotlivými členskými státy a Evropskou komisí o podpoře.

- **Jsmo jedni z 16 předložených projektů, dá se tedy nyní odhadovat, jaké jsou naše současné naděje na úspěch?**

Velmi dobré. Náš projekt má několik silných stránek, zejména ve výhodné lokalitě, rozvinuté domácí AI scéně a míře připravenosti, resp. schopnosti AI Gifactory rychle realizovat. Datacentrum Prague Gateway, ze kterého by se superpočítač rozšiřoval, se již dokonce začalo stavět. Zároveň máme velmi dobrou strategii. Navrhujeme vznik jedné společné AI Gigafactory pro celý region střední a východní Evropy (CEE), na které jsme připraveni spolupracovat s ostatními státy v regionu. Tento návrh jsme oficiálně představili Evropské komisi na jednání s vedením DG Connect 2. září v Bruselu. Komise tuto možnost výslovně schválila a vítá ji i z hlediska geografické vyváženosti v rámci EU.

Proto již nyní aktivně jednáme s dalšími členskými státy a náš návrh na spolupráci jsme oficiálně zaslali Polsku a v průběhu října bychom se měli na toto téma setkat. Do jednání obecně dáváme velké úsilí.

- **Co by konkrétně pro nás takový krok znamenal jak po stránce nároků, tak přínosů?**

Zřízení AI Gigafactory s tak mimořádným výpočetním výkonem by pro nás znamenalo zásadní přelom v našem postavení v oblasti digitálních technologií a umělé inteligence. Umožnilo by to trénovat AI modely s biliony parametrů, aplikovatelné ve zdravotnictví, školství, energetice, obraně i eGovernmentu. AI Gigafactory by znamenala obrovský rozvoj výzkumného potenciálu v AI i dalších oborech, přilákala ty nejlepší talenty a vědce z celé Unie a stala se i zároveň katalyzátorem rozvoje startupového a inovačního ekosystému, který kolem ní vznikne. Bude to mít pozitivní ekonomické dopady nejen na AI ekosystém, ale celý český průmysl.

- **V Mikulově jsme hodně mluvili o určité roztříštěnosti informací, jak a kde správně používat AI v rámci veřejné správy. Je reálná představa nějakého „centrálního“ školení zaměstnanců VS, nikoli aby získali informace o AI samotné, ale o tom, jak a do jaké míry ji ve VS používat (které kroky ano, které ne)?**

Ano, tato představa je nejen reálná, ale konkrétně připravovaná jako jeden z klíčových kroků naší národní strategie. Ve spolupráci s námi, Univerzitou Karlovou, Českou asociací umělé inteligence a společností Microsoft se pod Úřadem vlády připravuje projekt s názvem AI National Skilling Plan. Jeho cílem je nabídnout online školení pro všechny zaměstnance veřejné správy – nejen o tom, co je umělá inteligence, ale především jak ji smysluplně a bezpečně využívat v každodenní agendě veřejné správy. Tento projekt má ambici stát se centrálním bodem digitalizačního vzdělávání státu v oblasti AI a jeho spuštění plánujeme na podzim roku 2025.

- **Zvažuje stát třeba vytvoření AI laboratoře pro kvalitní testování a analytické práce nad návrhy řešení nástrojů pro práci státního sektoru v prostředí AI?**

Nad co neefektivnější spoluprací jednotlivých ministerstev v oblasti AI jsme vedli mnoho debat. Ministerstva jsou odlišná, každé má jiné agendy, datové zdroje i technickou připravenost, a tedy i různé potřeby při nasazení AI. Není tedy vhodné nasazovat stejný AI systém na sílu všude. Co ale má velký smysl, je jistě lepší koordinace, sdílení zkušeností a podpora vzájemné inspirace napříč institucemi. I proto jsme si založili pracovní skupinu Grémium AI ve veřejné správě, kterou koordinuje ministerstvo vnitra. Velmi užitečná je například nová databáze případů využití AI ve veřejné správě, kterou spustila Digitální informační agentura na adrese egovai.dia.gov.cz. Už nyní obsahuje desítky konkrétních AI use cases a její cílem je ukazovat, co už funguje a motivovat ostatní. Podobnou iniciativu připravuje rovněž prg.ai i pro soukromý sektor.

- **Z naší debaty vzešel i určitý problém nakládání s AI. Je v možnostech zaměstnavatele nějakým způsobem kontrolovat, jak vlastní zaměstnanci využívají AI (a to v pozitivním i negativním smyslu – zaměstnanec si tak může zefektivnit práci, ale mohl by i ohrozit výstup úřadu)?**

Je nezbytné vytvářet prostředí, kde se o využívání umělé inteligence otevřeně a zodpovědně komunikuje a zaměstnanci nemají obavu zaměstnavatele na rovinu informovat. Dnes je již nepochybné, že umělá inteligence může zaměstnancům významně usnadnit práci, zejména při zpracování velkého objemu dat, běžné administrativě či přípravě podkladů. Chceme, aby se AI stala běžnou a přirozenou součástí státní agendy, protože její přínos pro zvýšení efektivity je jednoznačný. Zároveň je však potřeba mít přehled o tom, jaké nástroje zaměstnanci používají a nastavit pravidla jejich využívání tak, aby nedocházelo zejména k úniku dat.



Ing. Jan Kavalírek působil před jmenováním náměstkem ministra průmyslu a obchodu na manažerských pozicích v soukromém sektoru, zejména v oblasti zdravotnických prostředků. Má zkušenosti s výzkumem, vývojem, výrobou i mezinárodním obchodem, podílel se na vybudování několika úspěšných společností. Rovněž působil jako zástupce ředitele certifikačního orgánu.

Jako expert na umělou inteligenci a medtech se podílel na evropských výzkumných projektech. Současně aktivně působí na Fakultě biomedicínského inženýrství ČVUT v Praze a pravidelně vystupuje jako keynote speaker na témata spojená s AI. Plynně hovoří anglicky a ve volném čase se věnuje boxu, lyžování, golfu či umění.

Na Ministerstvu průmyslu a obchodu se zaměřuje na umělou inteligenci a nové technologie, podporu startupového ekosystému, snižování administrativní zátěže pro podnikatele, posilování exportu českých firem a medtech sektor. Aktivně zastupuje Českou republiku v Radách Evropské unie pro mezinárodní obchod a telekomunikace a prosazuje modernizaci průmyslu prostřednictvím využití AI, inovací a digitalizace.

Na návrh ministra průmyslu a obchodu jmenovala v květnu vláda Jana Kavalírka vládním zmocněncem pro umělou inteligenci.



Používání volně dostupných online AI velkých jazykových modelů s sebou samozřejmě nese riziko úniku dat do zahraničí. I proto vláda, po konzultaci s NÚKIB, zakázala využívání nástroje DeepSeek ve státní správě, kde byla rizika nadměrně vysoká. Pokud chceme, aby AI pracovala s citlivými nebo neveřejnými daty, musíme implementovat řešení, která tato data neodesílají mimo systém. V této souvislosti jsou samozřejmě na místě i strategické debaty o vytvoření vlastního českého jazykového AI modelu, který by zajistil bezpečné, transparentní a efektivní využívání umělé inteligence ve veřejném sektoru.

• **Jak vnímáte zařazení AI do bezpečnostních dohledových nástrojů (fyzická bezpečnost – CCTV) včetně integrace s městskou policií? Mělo by v tomto směru existovat nějaké rozčlenění AI a jejího nasazení do VS?**

Využití umělé inteligence v oblasti fyzického dohledu, například v kamerových systémech ve veřejném prostoru, musí probíhat v přísném souladu s evropskou legislativou. AI Act v článku 5 výslovně zakazuje použití systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva, s výjimkou několika přesně vymezených situací – například při cíleném vyhledávání obětí únosů, při prevenci bezprostředního teroristického útoku, nebo při identifikaci osob již podezřelých ze závažných trestných činů.

Osobně mám za to, že článek 5 a zakázané systémy AI jsou dobře nastaveny a je nezbytné respektovat rozčlenění AI systémů na základě rizika a s ohledem na lidská

práva a ochranu soukromí. V rámci uvedených výjimek, které jsem zmínil, mám však za to, že je využití AI systémů pro zajištění vyšší bezpečnosti našich obyvatel přínosné.

• **Neuvažuje stát o vytvoření konsorcia ověřených dodavatelů AI v rámci kterého bude garantována bezpečnost dat a práce s AI především pro oblast veřejných zakázek?**

Určitě zvažujeme, jak podpořit bezpečné a důvěryhodné nasazení AI ve veřejné správě. Inspirací mohou být osvědčené modely z jiných oblastí, přičemž v oblasti AI by mohlo dávat smysl začít formou katalogu „compliance-ready“ dodavatelů, kteří splňují jasná kritéria v oblasti bezpečnosti dat a souladu s legislativou včetně AI Act. Takový nástroj by samozřejmě usnadnil orientaci a výběr důvěryhodných řešení pro státní správu.

• **Výstup z naší debaty na konferenci byl zřejmý, nemluvíme už o tom, jestli AI ve veřejné správě ano či ne, ale o tom, kde a jak. Jaké jsou podle Vás základní oblasti – činnosti, ve kterých by měla VS AI už nyní využívat? Případně Váš odhad dalšího vývoje?**

Nasazení umělé inteligence ve veřejné správě by vždy měla předcházet kvalitní data a procesy a následně digitalizace. AI systém je až konec řešení. Současně by AI neměla být jen formálním cílem, ale nástrojem, který řeší konkrétní úlohu a je za jejím použitím skutečný přínos, skutečný use case.

Už dnes vidíme první úspěšné příklady – na MPSV vytvořili systém Jenda, na Ministerstvu financí AI chatbot Adam pro grantovou agendu a na MPO připravujeme AI asistenta pro portál živnostenského podnikání. Nyní se připravují například nástroje pro zpracování žádostí podle zákona 106 na Úřadu vlády, kontrolu veřejných zakázek a automatizaci tvorby zadávací dokumentace na MMR, nebo třeba podporu rozhodování v agendě postupků na vnějšku. Jako strategický cíl pak vidím jednotný kontaktní portál veřejné správy vybavený AI nástroji, které občanům usnadní navigaci ve všech veřejných agendách a službách státu.

Microsoft proškolí v České republice 350 000 lidí v umělé inteligenci. Bud'te mezi nimi!

„80 % pracovníků po celém světě uvádí, že jim chybí dostatek času a energie na svou práci. 53 % manažerů říká, že produktivita se musí zvýšit.“

Umělá inteligence mění způsob práce. AI National skilling plan pomůže občanům získat základní dovednosti v oblasti umělé inteligence, aby byli úspěšní v budoucnosti.“



Michal Stachník

generální ředitel Microsoft Česká republika a Slovensko

Partnery jsou:

Úřad vlády ČR, Úřad práce ČR, Ministerstvo průmyslu a obchodu ČR, Ministerstvo školství, mládeže a tělovýchovy ČR, Univerzita Karlova, Univerzita Palackého v Olomouci, Národní pedagogický institut ČR, AI dětem, Česká asociace umělé inteligence, Digiskills, Prague Training Academy, K-Net, E-Bezpečí

EUDIW

Jedním z důležitých témat, kterým jsme se na konferenci e-government 20:10 v Mikulově věnovali, byla realizace Evropské peněženky digitální identity. Jedná se o projekt, který by nám měl umožňovat nejen prokazovat naši identitu na dálku (on-line), ale rovněž takto dokládat naše oprávnění, doklady o vzdělání a další důležitá fakta, a to vše napříč Evropou. Stát by se tak mělo ke konci roku 2026. I proto nás zajímalo, v jaké fázi se nyní nacházíme, zda je projekt v uvedeném termínu skutečně realizovatelný a hlavně, co nám doopravdy přinese, případně za jakých podmínek. Do diskuze se zapojili – Martin Mesršmíd, ředitel, DIA, Petr Budiš, generální ředitel I.CA, Pavel Kolář, Česká bankovní asociace a Jan Matuš, Vice President společnosti Aricoma.

Martin Mesršmíd v úvodu debaty navázal na své první vystoupení a znovu upozornil, že z pohledu realizace Evropské peněženky digitální identity bylo zcela zásadní, že vláda se přiklonila k formě koncese. Jedná se o postup, který doporučila poradenská společnost Ernst and Young jako variantu spolupráce soukromého a veřejného sektoru. Předpokladem je, že takto vysoutěžený poskytovatel elektronické peněženky bude po určitý čas mít hrazenou část nákladů, což bude podmíněno plněním určitých ukazatelů. Předpokladem je rovněž skutečnost, že poskytovatel peněženky bude mít nastaven obchodní model, kterým bude následně část nákladů pokrývat. Protože by se mělo jednat o projekt, u kterého nejen naše vláda předpokládá velký zájem veřejnosti, a tedy rozvoj, a především generování prostředků na provoz, považuje jej za životaschopný a ekonomicky udržitelný.

Petr Budiš potvrdil, že komerční sektor je s tímto modelem srozuměn a že to i koresponduje s určitou základní představou role státu a soukromých firem. Stát by se měl v tomto případě postarat o samotný back-office projektu, to je oblast, ve které ví, co je potřeba a jak to nastavit. Naopak na projektech jako elektronická občanka a dalších se ukázalo, že stát neumí dělat jednotlivým projektům řádný marketing. Je tedy dobře, že dá prostor komerčním společnostem, které jsou zvyklé své produkty prezentovat. Je totiž realistické předpokládat, že elektronická peněženka by měla být velkým přínosem jak pro občany, tak pro banky, ale i komerční sektor jako takový. Podstatné však je, aby obě strany byly schopny vyčíst jak náklady na realizaci projektu, tak jeho přínosy. Bude to byznys

model a pro ten je samozřejmě podstatné znát čísla na obou stranách.

Martin Mesršmíd připustil, že průzkum zájmu zatím vlastně neexistuje, protože není možné se ptát na to, zda by občané elektronickou peněženku chtěli používat, když jim ještě nejsme schopni představit celý rozsah jejího použití. Při těchto odhadech zájmu se tedy vychází z cíle Evropské komise, který říká, že v roce 2030 by mělo EIDW používat 80 % populace EU. Jak už zaznělo v samostatném vystoupení Martina Mesršmída, DIA dala, ve spolupráci s jednotlivými sektory, dohromady jakýsi prvotní seznam možného použití a tento seznam nadále rozšiřuje. Nicméně Martin Mesršmíd upozornil, že to, co bude digitální peněženku skutečně prodávat, nebudou zdaleka možnosti, které nabídne stát, a to především s ohledem na nízkou frekvenci s jakou občané řeší určité úkony vůči státu. To, co by mělo být skutečným lákadlem, bude nabídka komerčního sektoru, tedy bank, operátorů a dalších subjektů.

I Pavel Kolář, zastupující Českou bankovní asociaci, potvrdil, že je v podstatě se současným stavem spokojený, a to i proto, že vláda svým rozhodnutím potvrdila skutečnost, že bankovní sektor je již delší dobu v ČR podstatnou součástí řady digitalizačních projektů. K těm 80 % populace je potřeba říci, že se jedná o cíl, který bude nabíhat pozvolna. Bankovní sektor dal jasně najevo, že chce být určitým nositelem této myšlenky a stát se jakýmsi motívátorem rozvoje celého projektu. Neboť i když je přístup státu velice důležitý, jeho služby, jak bylo řečeno, v tomto směru tím největším lákadlem nebudou. Proto ČBA vnímá digitální peněženku jako impuls k nastartování řady pro-

cesů a digitalizačních aktivit, o kterých možná v tuto chvíli ještě ani nevíme.

K otázce určitého časového presu, když by měla být digitální elektronická peněženka k dispozici na konci roku 2026, Martin Mesršmíd zdůraznil, že to je termín podstatný pro spuštění funkční peněženky. Ale že to neznamená, že ve stejné chvíli bude k dispozici celá šíře možností jejího využití, tak jak se o tom bavíme. Je velice pravděpodobné, že tento náběh bude postupný. A určitě platí, že lákadlem budou nabídky komerčních subjektů, ale na druhou stranu právě možnost komunikace se státem, jakési „státní“ zastřešení, to je určitá důvěryhodnost a zároveň služba zajímavá pro všechny včetně soukromého sektoru. Nyní tedy je budována ona státní část peněženky, která bude sloužit právě k potvrzení různých atributů a identifikaci, které jsou v „držení“ státu. Zároveň je nutné připravit certifikační schéma, neboť nebude k dispozici jen jedna peněženka jednoho poskytovatele, ale postupně, zcela jistě, bude na výběr z většího množství produktů různých dodavatelů. A zároveň je ještě nutno dobudovat registr spoléhajících se stran. To jsou v tuto chvíli zásadní kroky pro samotný důvěryhodný provoz projektu. A navěšování služeb, které budou lákavé pro občany, to bude tedy teprve otázkou času.

Jan Matuš v tomto směru zdůraznil, že celý projekt je vlastně určitým impulsem pro další v jistém smyslu klientsky orientovaný rozvoj e-governmentu. Nařízení eIDAS 2.0 jednoznačně říká, že každý občan EU bude mít svou digitální identitu. A zcela zásadní změna paradigmatu je v tom, že občan bude mít tuto svou identitu skutečně u sebe a bude rozhodovat, jak tuto identitu a která konkrétní data použije, a to bez účasti státu, bez zásahu nějakého centrálního orgánu. To je opravdu něco nového, na co jsme nebyli doposud zvyklí. A právě proto je zřejmé, že bez soukromého sektoru, ale ani bez občanů a případné jejich kritiky a připomínek, není možné realizovat tento projekt. Kritiku projektu stát většinou vnímá negativně, ale v tomto případě je nutné to brát jako podnět k posunu správným směrem, tak aby se jednalo o uživatelsky přívětivý přístup. Celý problém samozřejmě umoc-

ňuje skutečnost, že se nejedná pouze o národní projekt, ale napříč celou Evropou (státy EU povinně, ostatní se mohou připojit).

Určitým zádrhelem odborných diskuzí byla otázka nekomerčního použití elektronických podpisů zdarma. Je to zakódováno přímo v nařízení eIDAS, nicméně bylo důležité například v rámci RVIS jasně vymezit, kde je ona hranice komerčního a nekomerčního použití. Protože samozřejmě platí, že i když je podpis poskytnut zdarma, musí jej ve výsledku někdo zaplatit a zároveň není možné poskytováním zdarma „nad míru“ narušovat trh. Nekomerční použití je tedy nyní vymezeno pro komunikaci mezi fyzickými osobami navzájem a mezi fyzickými osobami a státem. Představa je tedy taková, že pro tuto formu použití by certifikační autority měly poskytovat elektronický podpis občanům zdarma, a to recipročně za určitou „reklamu“, respektive odkazování na jejich služby. Petr Budiš potvrdil, že certifikační autority jsou s tím takto srozuměny a skutečnost, že peněženka nabízí jako povinnou součást jistou formu kvalifikovaného elektronického podpisu, je pro certifikační autority skutečně přínosem. Byla totiž nastavena jednotná úroveň napříč Evropskou unií, kdy tím uznávaným podpisem je právě kvalifikovaný elektronický podpis. Trochu problematické je samozřejmě ono dělení na komerční a nekomerční použití, což bylo ponecháno na lokálních orgánech. V rámci ČR se s řešením tohoto problému však DIA popasovala skutečně dobře. A pokud jde o rentabilitu, certifikační autority si v tomto směru udělaly kalkulace a rozbory a dospěly k názoru, že i takto nastaven dává projekt z jejich pohledu smysl.

V závěru diskuze pánové připomenuli důležitost otázky bezpečnosti projektu, a to jak v souvislosti se zachováním důvěry občanů v samotnou peněženku, tak samozřejmě v souvislosti s požadovanou změnou kryptografických algoritmů k 1.1. 2026, což při velikosti diskutovaného projektu je samozřejmě krok zcela zásadní. I jeho konkrétní řešení bylo ponecháno na rozhodnutí jednotlivých lokálních orgánů, takže DIA, certifikační autority a provozovatelé bezpečnostních systémů mají v tuto chvíli skutečně napilno.

PODEPISUJTE BUDOUCNOST: Digitalizace veřejné správy s důvěrou a jistotou

Na začátku září se Mikulov stal již tradičně centrem diskuse o budoucnosti eGovernmentu. Konference, která každoročně spojuje odborníky a zástupce ministerstev, obcí, měst i technologických partnerů, letos jasně ukázala: Česká republika stojí v bodě zlomu. Digitální služby už nejsou jen vizí, ale každodenní realitou.

Instituce hledají cestu k vyšší efektivitě a současně čelí stále přísnějším legislativním i bezpečnostním požadavkům. V centru této proměny stojí důvěra – bez ní by nebylo možné, aby lidé akceptovali plně elektronické procesy a aby úřady mohly garantovat, že digitálně podepsaný dokument má stejnou váhu jako ten listinný.

A právě důvěra je doménou První certifikační autority (I.CA), která je od roku 2001 akreditovaným poskytovatelem certifikačních služeb a dnes patří mezi přední evropské hráče v oblasti kvalifikovaných služeb vytvářejících důvěru podle nařízení eIDAS. Jen v roce 2024 vydala více než 168 milionů certifikátů pro elektronický podpis, téměř 300 tisíc vzdálených elektronických pečeti a přes 7 milionů časových razítek.

Certifikáty jako základ digitální důvěry

Elektronické certifikáty jsou klíčem k důvěryhodné komunikaci. Umožňují, aby si instituce a občané mohli být jisti, kdo dokument podepsal a že s ním nikdo nemanipuloval. To je zásadní nejen pro státní správu, ale i pro další obory, kde se pracuje s citlivými daty.

I.CA poskytuje kvalifikované certifikáty, které splňují požadavky eIDAS a zajišťují právní vymahatelnost elektronických úkonů napříč Evropskou unií. Pro úřady to znamená jistotu identity zaměstnanců i organizací a možnost nahradit zdoluhavé papírové procesy efektivními digitálními úkony.

Čipové karty: bezpečnost i přihlášení na jeden dotek

Digitální identita musí být chráněna nejen legislativně, ale i technicky. K tomu slouží čipové karty a hardwarové bezpečnostní moduly (HSM), vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru (QTSP), které bezpečně uchovávají kryptografické klíče.

Vedle bezpečnosti uchovávání a správy kryptografických klíčů spočívá jejich síla také v možnosti dvoufaktorové autentizace (2FA/2FF) – tedy kombinace toho, co uživatel ví (PIN) a toho, co má (čipová karta) s kryptografickými klíči. Úředníci se tak přihlašují k systémům i k citlivým datům bezpečněji a v souladu s požadavky NIS2. Stejně principy se následně uplatňují i v dalších oblastech, například ve zdravotnictví.

Podepisování odkudkoliv: vzdálené služby RemoteSign a RemoteSeal

Moderní trend digitalizace směřuje ke kvalifikovaným řešením „na dálku“. Proto I.CA vyvinula RemoteSign (vzdálený elektronický podpis) a RemoteSeal (vzdálenou elektronickou pečeť). Tyto služby zásadně mění způsob, jak mohou instituce pracovat s dokumenty – bez čipových karet nebo specializovaného hardwaru.

Podpisující už nemusí čekat, až se vrátí do kanceláře. Díky RemoteSign může podepsat dokument odkudkoliv – z pracoviště, z domova nebo i z jednání v terénu. Služba se snadno integruje do spisových systémů a umožňuje schvalování dokumentů rychle, bezpečně a v souladu s legislativou.



MÉNĚ PAPÍRU, VÍCE ČASU PRO PACIENTY

Nemocnice: když je důvěra pacientů na prvním místě

Principy digitální důvěry, které se osvědčily v úřadech, dnes pronikají i do zdravotnictví. Lékař potřebuje rychle a bezpečně přistoupit k dokumentaci pacienta. Využívá čipovou kartu, která není jen plastovým kusem s čipem, ale univerzálním klíčem. Umožňuje bezpečné přihlášení do nemocničního systému a díky dvoufaktorové autentizaci (2FA/2FF) splňuje i požadavky evropské směrnice NIS2 na kybernetickou bezpečnost.

Karta v sobě nese certifikát, který zajišťuje jednoznačnou identifikaci uživatele. Výsledkem je prostředí, kde mají citlivá zdravotnická data vysoký stupeň ochrany, přístup je auditovatelný a zároveň pohodlný. Lékař tak může bez obav podepisovat zdravotní dokumentaci přímo na oddělení – ať už jde o propouštěcí zprávu, nebo žádanku na další vyšetření.

Laboratoř: digitalizace v praxi

Další oblastí, kde digitalizace přináší zásadní změny, je laboratorní diagnostika. V první fázi projektu probíhá elektronizace toku zdravotnické dokumentace – od přijetí žádanky v laboratoři, přes zpracování biologického vzorku, až po vytvoření výsledku. Ten je opatřen elektronickou pečeti a časovým razítkem – pečeť důvěryhodně potvr-

zuje vznik dokumentu a časové razítko garantuje jeho neměnnost v čase. Výsledek je pak bezpečně a okamžitě doručen do ordinace v elektronické podobě.

V navazující fázi bude možné vystavit elektronickou žádanku přímo v ordinaci lékaře. Ta bude automatizovaně zpracována v laboratoři a výsledek se vrátí zpět do ordinace, kde bude nejen dostupný, ale i dlouhodobě důvěryhodně archivován. To přináší nejen úsporu času, ale i vyšší bezpečnost, eliminaci chyb a rychlejší péči o pacienta.

Partner pro digitální budoucnost

Veřejná správa i zdravotnictví dnes stojí před stejnou výzvou: jak propojit efektivitu, bezpečnost a dostupnost služeb. První certifikační autorita na tuto výzvu odpovídá komplexním portfoliem – od certifikátů, přes čipové karty a autentizaci, až po vzdálené služby a archivaci.

„Jsme přesvědčeni, že bez důvěry není digitalizace možná. Proto chceme být partnerem, na kterého se úřady i nemocnice mohou spolehnout při každém kroku – od prvního podpisu až po dlouhodobé uložení dokumentů,“ uzavírá Boris Kučera, ředitel segmentu veřejná správa.

Ing. Boris Kučera,
ředitel segmentu eGovernment



Gordic: Ohlédnutí za konferencí v Mikulově

V kulisách mikulovského zámku se opět sešli všichni ti, kterým leží na srdci digitalizace státu. A Gordic zde pochopitelně nemohl chybět. Bylo nám ctí být tradičním partnerem akce a potkat všechny tváře známé i neznámé, všechna setkání byla přátelská a inspirativní.

V průběhu konference vystoupil v hlavním sále Ladislav Mazač, ředitel odboru Strategický projektový management, s prezentací na téma: Co čeká spisové služby v roce 2026 z pohledu dodavatele. Ve své řeči poukázal na technický pohled na spisovou službu, ale i inspirativní paralely, ukazující, jak zásadní roli spisová služba hraje v moderní organizaci.

GINIS jako páteří systém digitalizace

Platforma GINIS je postavena na více než třicetileté zkušenosti a nabízí komplexní řešení nejen pro veřejný sektor. Platforma je dostupná jak v on-premise, tak cloud variantě, jehož standardizované zabezpečené rozhraní umožňuje rozšiřování pomocí tzv. kompozitních aplikací. Ty mohou vyvíjet certifikovaní partneři v rámci programu GPP, tj. Gordic partnerského programu, ale i další dodavatelé třetích stran.

Spisová služba je zde vnímána jako páteří informační systém, stěžejní pro digitalizaci, který zajišťuje komunikaci s tzv. eGOV systémy, jako jsou například základní registry, datové schránky, registr smluv atd.

Legislativa – řez obratlem

Ladislav Mazač přirovnal legislativní rámec dotýkající se Spisových služeb k řezu obratlem. Na tomto příkladu demonstroval, že provoz Spisové služby není v dnešní době regulován pouze zákonem o archivnictví a spisové službě, ale že je zde celá řada dalších regulací, které na spisovou službu mají dopad – GDPR, zákon o kybernetické bezpečnosti, cloud computing a další normy. Tyto požadavky kladou vysoké nároky na provoz Spisové služby.

Atestace spisové služby: krok vpřed

Gordic dne 24. června 2025 jako první podal žádost o atestaci spisové služby. Materiál, čítající přes 1200 stran, bude posuzován Českou agenturou pro standardizaci a výsledky se očekávají do konce letošního roku. Pro veřejnoprávní původce to znamená nutnost aktivní komunikace s dodavateli, seznámení se s novou legislativou a přípravu na změny s nasazením atestované Spisové služby – od revize spisového řádu po školení uživatelů.

Trendy, které nelze ignorovat

Dále Ladislav Mazač upozornil na několik klíčových trendů:

- **Cloudové služby:** GINIS je zapsán v katalogu cloud computingu v bezpečnostní úrovni 3;
- **Hybridní konverzní pošta:** Úspora času díky digitalizaci procesu odesílání dokumentů, autorizované konverzi atd.;
- **AI a machine learning:** Integrace do spisové služby pro automatizované zpracování dat;
- **Portál občana a design GOV.cz:** Důraz na uživatelskou přívětivost a propojení s dalšími systémy;
- **Standardizovaná rozhraní:** Automatizace a bezpečnost při integraci agendových systémů.



Co můžete udělat už teď?

Není radno podcenit přípravu. Ladislav Mazač doporučil kroky, které lze realizovat bez odkladu:

- Zařazovat dokumenty do spisu, provádět skartaci;
- Upravit spisový řád a plán;
- Připravit migrační schémata;
- Zajistit soulad s národním standardem;
- Školit uživatele.

Spisová služba není jen technický nástroj – je to páteř digitalizace. Atestace, nové legislativní požadavky a technologické trendy mění její podobu. Dodavatelé jako Gordic jsou připraveni pomoci s přechodem na nové standardy a jak říká Mazač: „Nejste na to sami.“

Ing. Zuzana Svobodová,
vedoucí oddělení marketingu



GORDIC

Řekněte sbohem manuálnímu IT! GREENLAKE INTELLIGENCE.

Mluvíme s generálním ředitelem HPE Tomášem Kubátem, který, trochu provokativně, říká: „Řekněte sbohem manuálnímu IT“, aby vysvětlil jednu z novinek z dílny HPE.

- **Tomáši, jak je to sbohem myšleno, řekněte více.**

Před časem jsem byl pozván jako host na IT konferenci, abych tam přednesl svůj key-note. V sále bylo asi 500 lidí – specialistů a manažerů IT – a měl jsem možnost jak na místě, tak i on-line získat jejich odpověď na můj jednoduchý průzkum během přednášky. Asi 90 % respondentů odpovědělo, že složitost IT prostředí stále narůstá, nebo je přibližně stejná (byť věcná témata se v čase mění). A jen 10 % se domnívalo, že nové technologie konečně IT zjednodušily.

- **No a co z toho vyplývá?**

Pro mě je to potvrzení určité saturace – uvažme, kolik nových technologií, konceptů nebo přístupů bylo uvedeno do IT v posledních měsících a letech. A vesměs měly za cíl poskytnout takové hodnoty užitečné pro business jako např. vyšší funkčnost, flexibilitu a jednoduchost. A přesto výsledek je, že IT se sice dobře rozvíjí, ale zjednoduší, a tím ani snadnější na zřizování a provozování IT služeb, to celkové prostředí příliš není. A naznačuje to, že co se dosud dělalo, je fajn, ale teď to chce něco zásadně kvalitativně nového.

- **Co nového máte na mysli?**

S tím právě teď přicházíme – je to GreenLake Intelligence. Místo complexity jednoduchost. Současná hybridní, stále složitější prostředí IT kladou velké nároky na IT týmy, které se starají o jejich provoz a rozvoj. Proto přicházíme se sítí doménově specifických AI agentů, kteří operují napříč hybridním prostředím IT, vzájemně spolupracují, sdílí kontext a znalosti. Analyzují, navrhují akce a realizují je. Představte si digitální AI experty a administrátory, kteří svému IT slouží 24x7.



- **Je to tedy vize, nebo produkt, nebo něco jiného?**

Kdybych teď neřekl, že je to produkt, mohl by si někdo myslet, že HPE jen sní o novém konceptu. A on to produkt skutečně je – přesněji je to doplnění o AI agenty u současných klíčových produktů HPE používaných v hybridním cloudu. To buď už je hotovo, nebo na tom pracujeme, záleží na konkrétním produktu. Ale současně je to koncept a strategické nasměrování firmy – je to inovace skutečně zásadního významu.

- **Takže s užitím GreenLake Intelligence se pak vše v IT děje samo?**

Skutečně nejde o pouhé expertní doporučení, ale o konkrétní automatizované akce, které systém provádí. Ale tam, kde je to potřeba, systém si vyžádá lidské schválení před provedením.

- **Jak spolu ti agenti komunikují?**

Agenti tvoří tzv. „agentní síť“ (agentic mesh). Ta jim umožňuje komunikovat, sdílet poznatky, koordinovat plány a udržovat kontext napříč různými doménami. Tato síť je

klíčovým konceptem, kde více doménově specifických velkých jazykových modelů (LLM) trénovaných na rozsáhlých datech HPE spolupracuje a sdílí kontext a znalosti. A to je umožněno díky protokolu Model Context Protocol (MCP), který standardizuje jazyk pro spolupráci mezi distribuovanými agenty.

- **Je to uzavřený systém, kde se uplatní jenom produkty HPE?**

Naopak, budujeme to jako otevřený systém, právě díky protokolu MCP. Smyslem je doplňovat, a ne nahrazovat, to, co již existuje a funguje. MCP zároveň umožňuje navázání na existující systémy a systémy třetích stran. Počítá se tedy s heterogenním prostředím IT.

- **Jak byste tedy GreenLake Intelligence popsal co nejvíce laicky?**

Asi bych řekl, že dosud GreenLake jako brand a koncept představoval „jednotný volant“ pro řízení, provozování a ovládání hybridního IT, tedy toho IT spočívajícího v kombinaci veřejného a privátního cloudu. To bylo a je k dispozici dosud. A s GreenLake Intelligence u takového volantu navíc už nemusí pořád sedět člověk. A tento volant funguje bez ohledu na to, zda příslušné technologie vlastníte, nebo je čerpáte jako službu.

- **Můžete dát příklad praktického užití?**

Představme si, že nás začne trápit zpomalená aplikace. Tehdy observability agent bude sledovat události v oblasti infrastruktury a aplikací, bude korelovat a analyzovat, osloví agenta networkingu, kde se identifikuje příčina (např. degradovaný síťový přepínač). Následně AI asistent předloží řešení ke schválení a po odsouhlasení se provede náprava. Takže žádné krizové porady, žádné dohady, jen rychlé řešení.

- **Máme očekávat, že teď všichni výrobci přijdou s podobným systémem?**

Za jiné výrobce nemohu mluvit. Ale mohu říct, že my v HPE jsme na hybridní cloud a hybridní IT vsadili už dávno a po celou dobu na tom pracujeme. Vyvinuli jsme technologie a máme obří objem získaných telemetrických dat, na kterých se systémy trénují. Není snadné, aby kdokoli rychle dosáhl stejné kvality.



Akvizice, která mění pravidla hry: HPE a Juniper Networks vstupují do nové éry síťových technologií

Představte si okamžik, kdy se trh s IT infrastrukturou začne přepisovat. Kdy akvizice není jen o rozšíření portfolia, ale o narušení zavedených hegemonických pozic a o definování nové budoucnosti. V rozhovoru s Michalem Svobodou, Country Managerem HPE Networking pro Českou republiku, Slovensko a Maďarsko, nahlédneme do zákulisí nedávné akvizice Juniper Networks společností HPE a poodhalíme, co tento krok znamená pro celý sektor a jaké překážky musel překonat.

Naskenujte QR kód pro více informací



- **Jak sám vnímáte GreenLake Intelligence?**

Jsem tím opravdu nadšen. Mám pocit, že to zahajuje novou éru IT. Jsem rád, že naše léta rozvíjená strategie a naše inovace se tak báječně potkávají s realitou na trhu.

Enters.cz

Hybridní cloud ve státní správě: už nejde o to JESTLI, ale JAK

Ještě před pár lety se vedla debata, zda státní správa vůbec potřebuje cloud. Dnes už otázka nezní jestli, ale spíše jakým způsobem k němu přistoupit. Trendy v oblasti IT jasně ukazují, že hybridní cloud – tedy kombinace státního, veřejného a on-premise prostředí – se stává přirozenou volbou pro české úřady i instituce.

Klíčové trendy ve veřejném IT

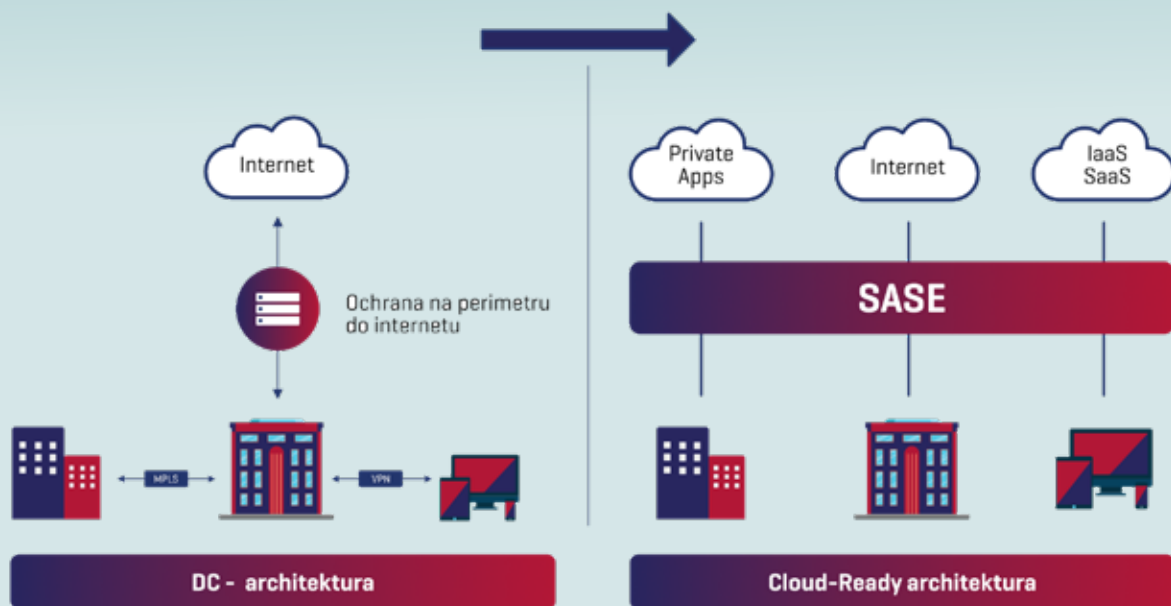
Bezpečnost zůstává absolutní prioritou. Tradiční pojetí ochrany založené na jediném firewallu mizí, protože aplikace a data se rozprostírají napříč cloudy a lokalitami. Ochrana se proto posouvá k principu „Bezpečnost všude“, tedy zabezpečení na všech úrovních – od aplikací, přes zařízení, až po síťovou infrastrukturu.

Hybridní způsob práce, který výrazně posílila pandemie, se stal standardem. Úředníci potřebují přístup k aplikacím odkudkoliv a ze všech zařízení, což komplikuje správu i zabezpečení. Do digitálního ekosystému navíc vstupu-

jí noví „uživatelé“ – IoT senzory, autonomní systémy nebo chytrá městská zařízení.

Další trend představuje přechod od izolovaných nástrojů k integrovaným platformám. Infrastrukturu dnes nelze efektivně provozovat jako soubor jednotlivých boxů. Automatizace, jednoduchost a přehledné řízení jsou nezbytné nejen pro správce IT, ale i pro koncové uživatele. Významnou roli přitom hraje umělá inteligence, která se stává součástí jak provozu IT, tak služeb pro občany.

Přechod od DC – středé architektury ke Cloud- ready





Uživatelé už dávno nesedí někde v centrále, ale jsou připojeni přes různá prostředí (doma, na cestách) a především aplikace a jejich data jsou provozovány v různých datových centrech, privátních či veřejných cloudech a konzumovány různými způsoby včetně IaaS, PaaS, SaaS, apod.

Hybridní cloud se ukazuje jako nejefektivnější cesta, jak tyto trendy a nově vznikající požadavky propojit s využitím konceptů typu SASE (Secure Access Service Edge), včetně technologie SD-WAN či SSE.

Globální i lokální perspektiva

Podle analytiků Gartneru přesáhnou celosvětové výdaje na veřejný cloud do konce roku 2025 částku 723 miliard USD, což znamená růst o více než 21 %. Zásadnější ale je, že až 90 % organizací přijme do stejného roku hybridní cloud jako cílový model.

Do popředí se přitom dostává i tzv. repatriace – návrat aplikací a dat zpět z veřejného cloudu do privátních nebo on-premise prostředí. Podle průzkumů tak činí až 83 % firem. Důvody jsou jasné: nepředvídatelné náklady, požadavky na bezpečnost a datovou suverenitu, potřeba fungovat nezávisle v krizových situacích nebo provoz specializovaných aplikací, včetně AI. Pro státní správu to znamená jediné – spoléhat výhradně na jeden model je riskantní.

Role státního cloudu v ČR

V českém prostředí má klíčovou pozici SPCSS (Státní pokladna Centrum sdílených služeb), která provozuje vládní cloudovou infrastrukturu. Ta poskytuje:

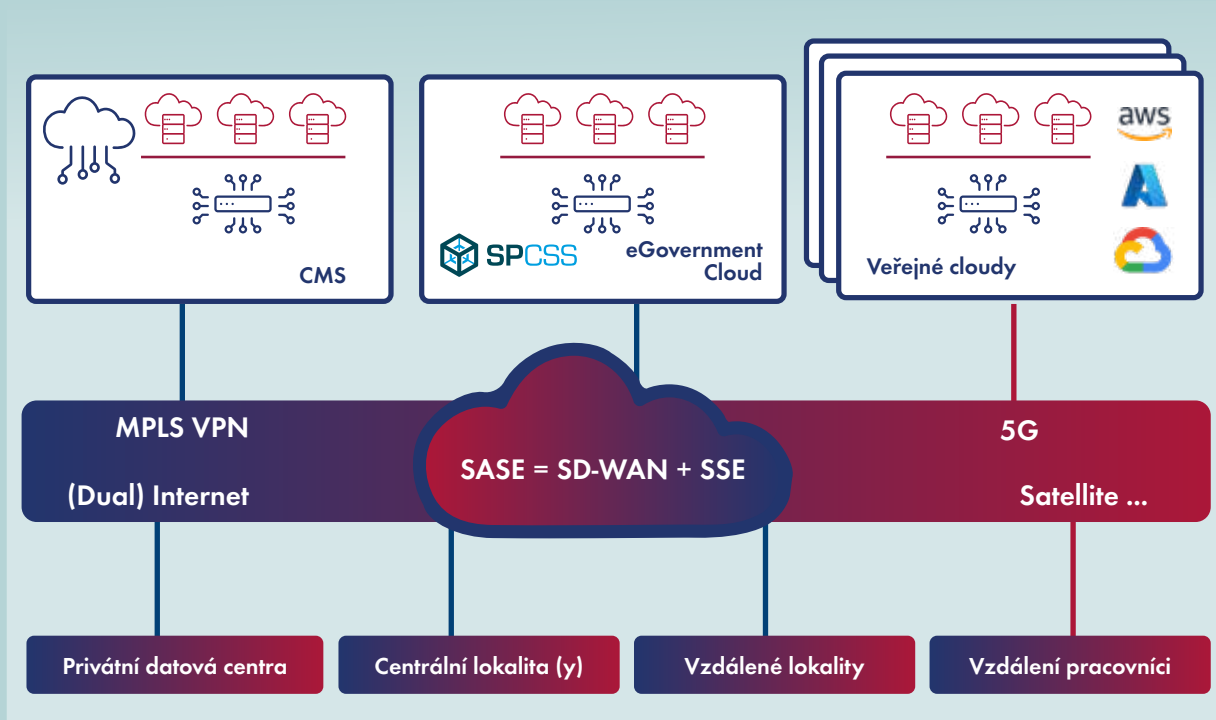
- Bezpečnost garantovanou státem,
- Soulad s legislativou a regulacemi,
- Lokální umístění dat v ČR,
- Vyšší míru kontroly a provozní kontinuitu.

Státní cloud se tak stává základním stavebním kamenem hybridního přístupu, který lze dále rozšiřovat o veřejné a lokální prostředí.

Přínosy hybridního cloudu pro státní správu

Hybridní cloud dokáže nabídnout to nejlepší z obou světů – flexibilitu veřejného cloudu a stabilitu státní infrastruktury. Mezi hlavní přínosy patří:

- Flexibilní komunikační architektura propojující různé domény (Azure, SPCSS, on-prem),
- Vysoká dostupnost a nezávislost na konkrétních operátorech,
- Rozšiřování výkonu podle potřeby,
- Integrované bezpečnostní služby – od integrace firewallů po nativní WAN segmentaci,
- Připravenost na budoucí rozvoj, včetně SD-WAN pro vzdálené úřady.



Nová architektura sítí

Hybridní cloud přináší tlak na novou síťovou architekturu, která musí být připravena na cloud. To znamená rychlejší nasazení a snadnější migrace, vyšší úroveň automatizace a centrální řízení, analytiku i SLA monitoring. Současně je nezbytné optimalizovat propojení mezi státními, veřejnými a lokálními cloudy.

Strategické ukotvení

Hybridní přístup není jen technologickou volbou, ale i součástí dlouhodobých strategických plánů. České úřady se mohou opírat o klíčové dokumenty jako Digitální Česko, Informační koncepce ČR, Strategický rámec Národního cloud computingu nebo Národní strategii kybernetické bezpečnosti 2026+. Tyto materiály jasně stanovují směr – bezpečné, interoperabilní a efektivní digitální služby pro občany.

Závěr

Česká státní správa už neřeší, zda cloud potřebuje. Otázka dnes zní: Jak jej správně navrhnout a integrovat? Spojení státního cloudu se službami veřejného i privátního prostředí nabízí cestu k bezpečné, flexibilní a škálovatelné infrastruktuře, která obstojí i v krizových situacích. Úspěch hybridního modelu však bude záviset na pečlivé integraci sítí, bezpečnostních opatření a schopnosti udržet kontrolu nad daty. A právě zde má prostor osvědčený partner, jakým je Simac Technik ČR, a.s. – specialista na komunikace, infrastrukturu a spolehlivá řešení nejen pro veřejný sektor.

Pavel Křížanovský
Vedoucí oddělení infrastruktury
Simac Technik ČR, a.s.

Oracle EU Sovereign Cloud

Nabídka cloudových služeb, určená pro zákazníky z EU, která organizacím z komerčního a veřejného sektoru umožňuje umístit citlivá data a aplikace do cloudu v souladu s požadavky datové suverenity EU. K dispozici již od roku 2023.



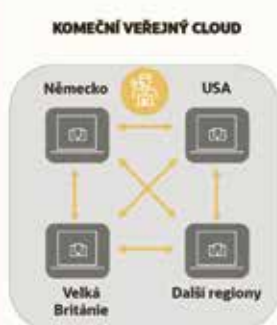
Suverénní cloud EU navržený a provozovaný pro digitální suverenitu EU a soukromí vašich dat. EUSC je 100% vlastněný legální entitou z EU.



Nabídka služeb a za stejnou cenu jako v komerčním cloudu Oracle (žádný „příplatek za digitální suverenitu“).



Kompletní portfolio služeb jako v komerčním cloudu. S garantovanou digitální suverenitou navíc (například AI s garantovaným umístěním v EU).



Fyzická a logická izolace

Fyzická a logická izolace

Služba Oracle EU Sovereign Cloud se nachází ve fyzicky izolovaném prostoru datového centra a nemá páteřní síťové (a ani jiné) připojení k jiným cloudovým regionům společnosti Oracle.

Provoz EUSC striktně oddělený od komerčního

Provoz a zákaznická podpora EUSC jsou v rámci EU prováděny týmy, které jsou složeny výhradně z občanů EU. Je přísně oddělený od komerční části.

POPRVÉ A NAPOSLED

(s využitím TZ-DIA)

První možnost využít eDoklady při volbách do Poslanecké sněmovny přinesla rekordní zájem veřejnosti, ale i vážné technické problémy. V průběhu volebního víkendu se ukázalo, že digitální ověřování totožnosti je pro občany atraktivní. Současně se ale objevily komplikace, které ovlivnily část uživatelů při aktualizaci digitálních dokladů. Za vzniklé potíže se DIA omlouvá.

POPRVÉ U VOLEB

Během prvních 4 hodin voleb byl zaznamenán rekordní počet přihlášení do eDokladů přes NIA (přes 1,5 milionu). Problémy se objevily primárně v části aplikace, která zajišťuje aktualizaci samotných digitálních dokladů. V těchto chvílích docházelo k přetížení, které ovlivnilo dostupnost služby pro uživatele, kteří neměli aktualizovaný doklad.

Kolem šesté hodiny došlo k nasazení úpravy aktualizace dokladů, která však z počátku nebyla stabilní. Systém se stabilizoval až v dalších hodinách, druhý den již fungoval bez zásadních omezení. Systém NIA, který zajišťuje přihlášení, prokázal, oproti předchozím zkušenostem, po spuštění nového cloudového datového centra vysokou stabilitu a docházelo pouze k drobnému zpomalení při zmíněné extrémní zátěži.

Aplikace eDoklady prošla před volbami testováním, skutečný provoz ale přinesl specifickou situaci. Tou byl mimořádně koncentrovaný nápor aktualizací požadavků v krátkém časovém okně, který nebylo možné v současných testovacích podmínkách plně nasimulovat.

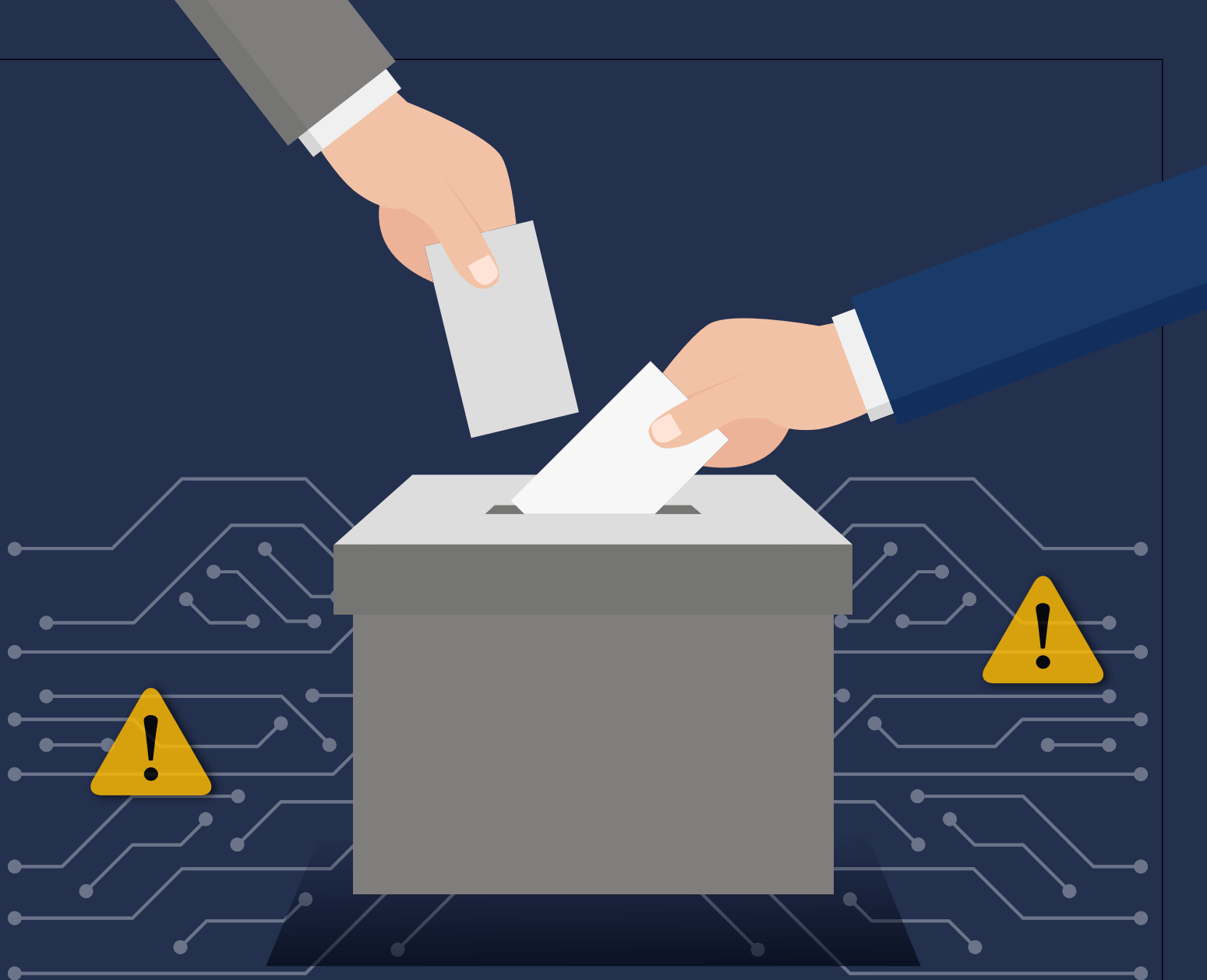
„Došlo k nesprávnému odhadu a testování na tuto zátěž. Zájem o eDoklady byl velký, což nás velmi potěšilo a velmi nás mrzí to, že se nepodařilo zájem pokrýt kapacitou systému,“ uvedl ředitel Martin Mesršmíd, který zároveň v reakci na nastalou situaci nabídl svou rezignaci vicepremiérovi pro digitalizaci Marianu Jurečkovi.

NAPOSLED VE FUNKCI

Ministr a vicepremiér pro digitalizaci Marian Jurečka přijal rezignaci ředitele Digitální a informační agentury Martina Mesršmída, a to k 23. říjnu 2025. Mesršmíd nabídl svou funkci právě během „volebního“ víkendu, v reakci na to, že se DIA potýkala s problémy eDokladů, které některým občanům znepříjemnily využití možnosti prokázat se digitální občankou u volebních komisí při volbách do Poslanecké sněmovny.

Martin Mesršmíd byl jako první ředitel Digitální a informační agentury u samotného zrodu úřadu. „Vznik Digitální a informační agentury (DIA) je v posledních letech možná jedním z nejvýznamnějších kroků, který dodá potřebný impuls digitalizaci státní správy. Před vznikem DIA řešily jednotlivé resorty digitalizaci své agendy odděleně a bez větší koordinace,“ napsal Mesršmíd ve výroční zprávě agentury za rok 2023.





Za prvních 8 měsíců fungování v roce 2023 se povedlo úspěšně posunout spoustu projektů. Agentura připravila novou mobilní aplikaci eDoklady, představila novou podobu Portálu občana, dokončila kontejnerizaci NIA, začala pracovat na Registru zastupování, koordinovala postupné naplňování Zákona o právu na digitální služby, pracovala na Zákonu o správě dat a věnovala se aktivně i evropské digitální peněženice, na jejímž zavedení doteď pracuje.

V průběhu roku 2024 došlo k vybudování kompetenčních center a k obsazení pozic špičkovými odborníky. NIA a většina dalších služeb přešly pod jednotnou státní doménu gov.cz, což vedlo ke zvýšení kybernetické bezpečnosti a uživatelské přívětivosti. Realizovaly se rozvojové projekty na registru práv a povinností (RPP), kdy se

jednalo zejména o Registr zastupování, Navigační systém Katalogu služeb, Import údajů z datového slovníku a převod dat z Registrační autority základních registrů.

„Byl to dynamický rok, který přinesl další rozvoj státní digitální infrastruktury. DIA systematicky propojuje data státu, čímž dochází ke zjednodušení, procesnímu zrychlení i prevenci chybivosti. Byl to rok úspěšný, i když v mnoha ohledech těžký. DIA je již pevně etablovaným úřadem, lídrem v oblasti digitalizace celé státní správy a zasazuje se o hladkou komunikaci mezi státem a občanem,“ uzavíral své úvodní slovo Mesršmíd ve zprávě o činnosti za rok 2024.

NAŠI KLIENTI UMÍ VYHRÁVAT



Premium

Sázíme na vypilovanou techniku. Jdeme vám naproti s individuální obsluhou a exkluzivními službami. Vy se tak můžete soustředit na své disciplíny. Chtějte vždy to nejlepší.

Premium linka +420 499 900 900 | www.csobpremium.cz