Egovernment

elektronizace veřejné správy

Digitalizace?
ALE UŽ!

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: Karolína Modranská

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.

HPE GreenLake

Modernize with the cloud that comes to you

Should you move all your apps and data to the cloud? You can choose not to choose with HPE GreenLake—the platform that brings the cloud to you.

Visit **GreenLake.HPE.com**

HPE GREENLAKE | EDGE-TO-CLOUD PLATFORM

Konference e-government 20:10 – jubilejní i třeskutá

Magazín Egovernment uspořádal na zámku Mikulov počátkem září již po patnácté konferenci e-government 20:10. Jubilejní ročník se nesl ve znamení „nabitého" programu a rekordní účasti. Díky romantickým zámeckým prostorám i nádhernému počasí byli všichni s návštěvou spokojeni a časová vytíženost a v některých chvílích přeplněnost sálů nijak nevadily. Krom samotných účastníků v sálech mohli celý průběh konference sledovat i diváci streamu.

Konference dodržuje tradiční režii, rozdělení do dvou dnů propojených společenským večerem a členění na plenární jednání i tematické sekce. Zahájení je tradičně v rukou těch, kteří poskytují konferenci svoji záštitu, respektive jejich zástupcům, tedy vicepremiéra pro digitalizaci a ministra pro místní rozvoj, hejtmana Jihomoravského kraje a starosty města Mikulov. Zatímco zastoupení Ivana Bartoše jeho náměstkem **Ondřejem Profantem** a zastoupení hejtmana zastupitelem Jihomoravského kraje **Ivo Vašíčkem** nebylo ničím neobvyklým, reprezentace Mikulova byla na konferenci premiérová. Letos poprvé v této roli vystoupila nová starostka Mikulova paní **Jitka Sobotková**, která krom přivítání účastníků ve „svém" městě jubilejní ročník zahájila slavnostním „zapálením" ohně.

I další část plenárního programu prvního dne konference byla očekávána s napětím, a to především s ohledem na skutečnost, že teprve od 1. 4. 2023 funguje **Digitální informační agentura**. Prvním prezentujícím byl její ředitel **Martin Mesršmíd**, který ve své prezentaci nastiňoval důležitost, určení, další směrování agentury a především pak cíle, které si klade v oblasti dalšího vývoje elektronizace veřejné správy. V diskuzi odpovídal na dotazy směřující ke kompetenčním centrům, firmám realizujícím projekt eDoklady, vzdělávání veřejnosti i zaměstnanců veřejné správy, napojení AIS k referenčnímu rozhraní datového fondu a podrobnosti okolo projektu REZA. Záznam celé diskuze, stejně jako ostatních vystoupení na konferenci, můžete shlédnout na www.egovernment.cz v sekci MIKULOV 2023.

Na Martina Mesršmída navázal možná ještě výbušnější prezentací prezident Hospodářské komory ČR a prezident ICT Unie **Zdeněk Zajíček**. Jeho vystoupení bylo diváky vyhodnoceno jako nejpoutavější v rámci úvodní části. Propojil v něm nejen zaměření obou institucí, které reprezentuje, ale na základě jejich znalostí a informací upozornil na důležité, a v určitém smyslu krizové, momenty. Z pohledu e-governmentu se jedná o zásadní apel na dodržení termínu pro spuštění **zákona o právu na digitální službu** jakožto „digitální ústavy". I proto jsou důležitá některá upozornění, která v rámci tohoto vystoupení zazněla.

Atmosféru jsme následně trochu zklidnili, když jsme na podiu vytvořili improvizované Studio Egovernment, tedy diskuzi tentokráte na téma **eWALLET/eDoklady**. Chtěli jsme si především ujasnit, jaký je rozdíl a proč máme evropský a národní projekt vedle řady komerčních, co je podstatou a kam v oblasti elektronických dokladů směřujeme. K diskuzi jsme přizvali ředitele DIA **Martina Mesršmída**, zástupce ČSOB **Pavla Koláře** a generálního ředitele a předsedu představenstva I.CA **Petra Budiše**. Zde diváky zajímala především otázka povinností jednotlivých úřadů financovat eWallet a samozřejmě pak technická podstata online či offline prokazování identity, informační kampaně v této oblasti, termíny realizace a možností využití i pro komerční sféru atp. I tato diskuze je v záznamu k dispozici na uvedených webových stránkách.

„JSME NA KŘIŽOVATCE – MÁME OBROVSKÝ DEFICIT NEJEN V DIGITALIZACI, ALE I OSTATNÍCH OBLASTECH."

„TENTO STÁT NEBUDE FUNGOVAT, POKUD SE DRAMATICKY NEZDIGITALIZUJE – NEZTRÁCEJME ČAS DISKUZEMI O TOM, KTERÝ ÚŘAD MÁ CO DĚLAT, ALE UDĚLEJME TO!"

„ČEKÁ NÁS DESETILETKA, KDY BUDEME MUSET DO INFRASTRUKTURY INVESTOVAT V ŘÁDECH TISÍCŮ MILIARD!"

„NEJSEM ŠŤASTNÝ Z TOHO, JAK DIA VYPADÁ, A S KONCEPTEM, JAKÝM SE V TUTO CHVÍLI REALIZUJE, SE NEZTOTOŽŇUJI."

Zdeněk Zajíček

Protože i z pohledu výše uvedených projektů je velice důležitý kvalitní, a především bezpečný cloud, následovaly prezentace ředitele technického úseku SPCSS pana Jiřího Kruly **o připravenosti SPCSS poskytovat státní cloud** a Milana Habrcetla z CISCO o **cloudové bezpečnosti.** Úplný závěr dopolední části pak obstaral ředitel odboru regulace NÚKIB Adam Kučínský se svou **Zprávou o aktuálním stavu směrnice NIS2 a nového zákona o kyberbezpečnosti.** Vzhledem k obsahu a aktuálnosti to byla druhá nejpopulárnější prezentace z dopolední části.

Odpolední program konference se tradičně rozděluje do dvou sekcí, a to **Egovernment** a **Kyberbezpečnost**. O narůstající důležitosti KYBEZ svědčí i skutečnost, že prezentace na toto téma, kromě samostatné sekce, zabíraly téměř polovinu té věnované Egovernmentu. Samotná vystoupení pak pokrývala širokou oblast – **vládní dohledové centrum, SOC v prostředí státní správy, NIS2, bezpečnost cloudu, ochranu webových aplikací, e-doklady, spisovou službu, umělou inteligenci, platformu Golemio či eGC kalkulátor.**

Večerní program je vždy jakousi odměnou účastníkům za jejich „výdrž". Přece jen je celý konferenční den velice náročný, a tak i letos účastníky pozvala na zámecké nádvoří kapela **B.LUES** a **Bohouš Josef**, v jejichž podání zazněla řada hitů předních světových interpretů. Atmosféra letního večera byla fantastická a účastníci si koncert pod hvězdami vychutnali.

Druhý konferenční den je obvykle monotematický a více diskuzní a komorní. Letos jsme jako téma zvolili problematiku spisových služeb, otázky nového zákona o spisových službách a především problematiku atestací. K diskuzi a prezentacím usedli: **Petr Vokáč**, vrchní ředitel sekce legislativy a státní správy, MV ČR; **Karel Trpkoš**, vrchní ředitel sekce informačních technologií, MPSV; **Petr Stiegler**, Česká agentura pro standardizaci; **Tomáš Bezouška**, INADVISORS, **Ladislav Mazač**, Gordic.

I zde kromě samotných prezentací museli vystupující odpovídat na otázky z publika. Ty směřovaly velmi často na Českou agenturu pro standardizaci, a to především ohledně personálního zajištění atestací, cen za atestace, principu a postupu atestací, problematiky open-source spisových služeb, aktualizace zákona atp. I zde platí, že záznam celé diskuze je vám k dispozici.

Diskuze o spisových službách zakončila nejen druhý den, ale i celý 15. ročník konference, který byl realizován pod záštitou **Ivana Bartoše**, vicepremiéra pro digitalizaci a ministra pro místní rozvoj, **Jana Grolicha**, hejtmana Jihomoravského kraje, **Jitky Sobotkové**, starostky Mikulova, a za podpory MV ČR, DIA, NAKIT, SPCSS, CISCO, EVIDEN, GORDIC, IBM a řady dalších partnerů, kterým děkujeme.

Veškeré prezentace, videozáznamy a fotografie z 15. ročníku konference e-government 20:10 naleznete na www.egovernment.cz v sekci MIKULOV 2023.

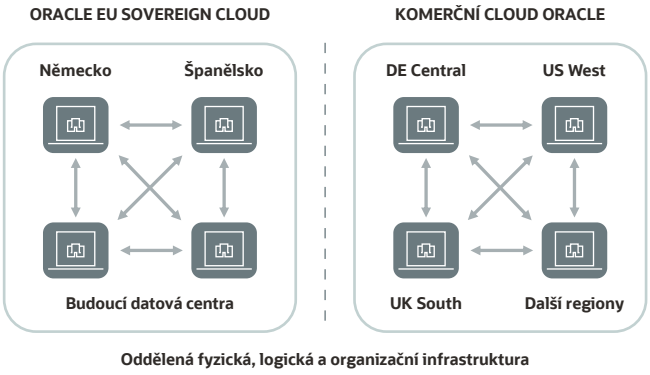
ORACLE

Oracle EU Sovereign Cloud

Cloudové prostředí, zaručující umístění a správu vašich dat v rámci Evropské Unie

Oracle EU Sovereign Cloud (EUSC) umožňuje zákazníkům z veřejného i komerčního sektoru umístit svoje citlivá data a aplikace do cloudového prostředí, které je plně v souladu s regulačními pravidly EU. EUSC poskytuje ještě vyšší míru kontroly nad soukromím a bezpečností vašich citlivých dat.

Datová centra Oracle EU Sovereign Cloud jsou umístěna a provozována pouze v rámci zemí EU. Tato datová centra jsou logicky, fyzicky a organizačně kompletně oddělena od komerčního cloudového prostředí.



Oracle EU Sovereign Cloud je postavený na stejných technologických principech a poskytuje kompletní portfolio cloudových služeb jako jeho komerční varianta. Migrace řešení z komerčního cloudu Oracle do EUSC a naopak je proto velmi rychlá a bezproblémová. Ceník cloudových služeb EUSC se nijak neliší od komerčního. Úroveň podpory a SLA v EUSC je stejná jako v komerčním prostředí.

Kontaktujte nás

https://www.oracle.com/cz/
Oracle Czech
Telefon: +420 220437006

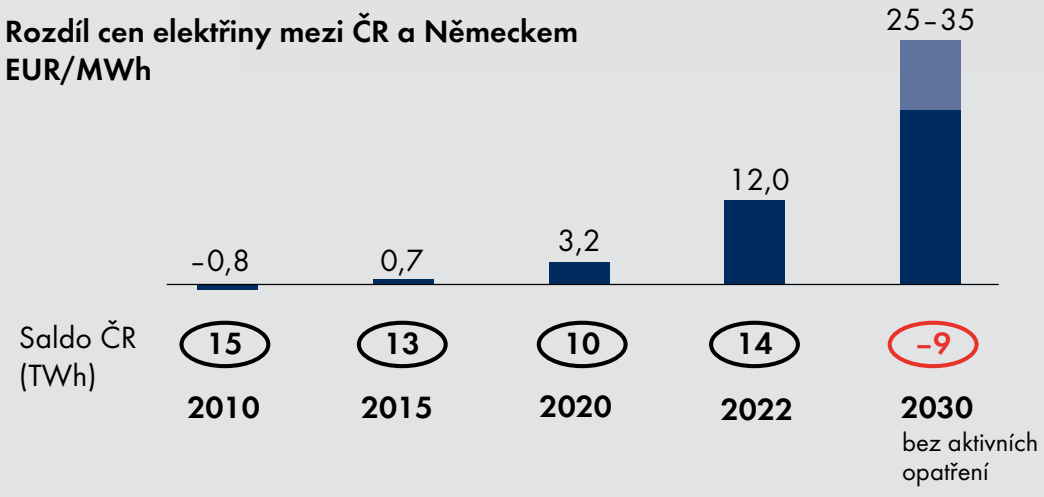
Stav a naplňování zákona o právu na digitální služby

Prezident Hospodářské komory ČR a prezident ICT Unie, Zdeněk Zajíček, upozornil, že to bylo poprvé v roce 2017, kdy právě zde na konferenci v Mikulově veřejně vystoupil s myšlenkou, že „občan má právo na poskytnutí digitální služby". A z jeho pohledu je velice potěšující skutečnost, že příslušný zákon byl nakonec přijat obrovskou většinou. Je zároveň příznačné, že zpravodajem tohoto zákona a osobou, která jej „protahovala" Poslaneckou sněmovnou, byl Ivan Bartoš, dnes vicepremiér pro digitalizaci. O to více alarmující je skutečnost, že Z. Zajíček musí s tímto tématem v roce 2023 vystoupit jako s apelem na jeho realizaci.

Zdeněk Zajíček před rokem usedl, podle svých vlastních slov, do „horké" židle koordinátora energetické krize a jednal o zastropování cen energií tak, abychom zvládli cenovou energetickou krizi. Při této příležitosti si uvědomil, že není možné se dívat „pouze" úzce na elektronizaci samotnou, ale vnímat všechny souvislosti. Je to o to důležitější, že jsme podle jeho slov **na křižovatce**. Máme totiž obrovský deficit nejen v digitalizaci, ale i v řadě ostatních směrů. Konkrétně nám schází odpovídající investice do strategických oblastí, za které považuje **energetiku, dopravu, trh práce, bydlení, ale i vzdělávání, výzkum a inovace**. To vše jsou dlouhodobě podkapitalizované oblasti, do kterých je nutné investovat. Z pohledu naší konference je podstatné, že ve všech těchto oblastech hraje zásadní roli ICT. Dá se říci, že bez informačních technologií nelze v těchto strategických oblastech nic postavit ani provozovat. Proto je nutné si uvědomit, že tento **stát nebude fungovat bez toho, aniž by se dramaticky nedigitalizoval**. Podle Zdeňka Zajíčka **bychom tedy neměli ztrácet čas diskuzemi o tom, který úřad bude co dělat, místo toho, abychom to udělali**. Je však nutné, aby v tomto směru panovala široká shoda.

I proto byl vyzván premiér, aby zahájil jednání s prezidentem republiky a představiteli politických stran a hledala se široká politická dohoda napříč politickým spektrem, protože chceme-li být konkurenceschopní, pak nás čeká **desetiletka, kdy budeme investovat do infrastruktury v řádech tisíců miliard**, a takový krok není realizovatelný bez široké politické shody.

... a bez aktivních opatření povede k deficitní bilanci a vysokým cenám



Tuto potřebu demonstroval Zdeněk Zajíček právě na oblasti energetiky. Podle podkladů, které má Hospodářská komora ČR k dispozici, by naše energetická bilance, kterou máme nyní přebytkovou, mohla už v roce 2030 být výrazně deficitní (viz graf). To by následně mělo zásadní vliv na cenu energií, kterou budeme v takovém okamžiku mít výrazně vyšší než sousední státy, které například vytvořily alianci na získávání energie z větrných elektráren. Pokud nepostavíme infrastrukturu, kterou bychom se i my k těmto elektrárnám připojili, nebudeme konkurenceschopní a nebudeme schopni vyvážet a prodávat naše zboží, protože budeme limitováni drahou energií. Podobně vážné to je i v resortu dopravy. Pokud nebudeme mít dostatečnou dálniční síť, pokud nebudeme mít vysokorychlostní tratě, nebudeme moci konkurovat okolí.

CO VŠECHNO CHYBÍ

Z průzkumu Hospodářské komory ČR, Svazu průmyslu a dopravy ČR a Konfederace zaměstnavatelských a podnikatelských svazů ČR ve spolupráci s IPSOS zaměřeného na strategické investice vznikl přehled toho, co je z pohledu podnikatelů možné považovat za nejvážnější faktory, které ohrožují strategické investice:

- **dlouhé povolovací procesy 55 %;**
- **chybějící vize státu 45 %;**
- **složitá legislativa neprovázaná se strategickými dokumenty 43 %;**
- **často se měnící legislativa 27 %;**
- **nedostatek pracovní síly 26 %.**

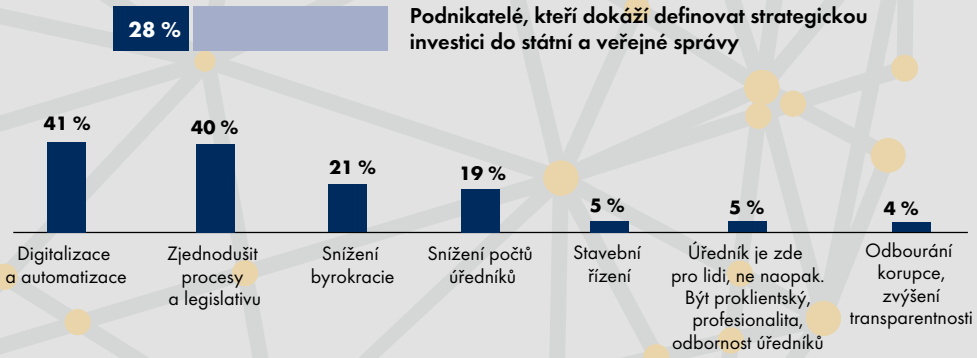
Je zřejmé, že se nedá vše napravit najednou. Je však nutné si připustit, že **to, že pracujeme, ještě neznamená, že to děláme skutečně efektivně** a dostatečně rychle. **Jsme sice uprostřed Evropy, ale mohli bychom se stát jejím skanzenem.** Není totiž zřejmý jediný důvod, proč by v tuto chvíli měla jakákoliv další firma, například z USA, zakládat v ČR pobočku a cokoliv tu vyrábět. Bude to zde mít drahé a komplikované oproti jiným státům v okolí. Jsme tedy ve velkém ohrožení, a právě proto se musíme dohodnout a prosadit klíčové změny. Je to odpovědnost politické reprezentace.

Z uvedeného průzkumu Hospodářské komory ČR dále vyplývá, že podnikatelé považují za nejpotřebnější strategické investice do digitalizace a automatizace ve veřejné správě. I proto Zdeněk Zajíček zdůraznil, že odkládat zákon o právu na digitální služby z termínu 1. 2. 2025 na jakýkoliv pozdější nechce a udělá vše pro to, aby se tak nestalo, přičemž zdůrazni, že **nepotřebujeme stavět žádné další úřady, máme jich dost, potřebujeme začít dělat.**

POTŘEBA POLITICKÉ SHODY

Téma elektronizace veřejné správy by mělo být apolitické, respektive by na něm měla panovat shoda napříč politickým spektrem. Bylo tomu tak například i v roce 2006, kdy jsme zaváděli Czech POINTy, datové schránky či základní registry. I proto tyto projekty stále fungují a můžeme se o ně dodnes opírat, a dokonce se jimi chlubit jako tím nejlepším, co v rámci digitalizaci máme. Právě proto Zdeněk Zajíček vždy dbal na širokou politickou dohodu, ať už šlo o zákon o právu na digitální službu, o digitální identitu či velmi komplikovanou a složitou věc, jako je digitalizace stavebního řízení. V tomto případě pro něj hlasovalo 188 poslanců, neboť všichni věděli, proč se o této problematice hlasuje a co je cílem. Jak zdůraznil, domníval se, že když o tom celá politická reprezentace věděla a měla možnost dva a půl roku diskutovat a zasahovat, je to dostatečně silný základ pro úspěšnou realizaci v termínu 1. 7. 2024. Nechápe tedy, proč nová politická reprezentace koncept, který nebyl tajný, ale veřejně obhajovaný, nyní ruší. Má velikou obavu, že kvůli tomu termín 1. 7. 2024 opravdu nestihneme a digitalizace stavebního řízení určitě nebude v té podobě, jak jsme si ji představovali. Přitom digitalizace a automatizace zrovna u povolování staveb je klíčová věc, bez které se určitě nepohneme dál.

Strategické investice: investice do státní a veřejné správy



JAK NAPLNIT ZÁKON?

Zákon o právu na digitální služby je nazýván i digitální ústavou. Obsahuje klíčová ustanovení pro elektronizaci veřejné správy, například to, že OVM zveřejňují elektronické formuláře, které se po prokázání totožnosti předvyplní. To ale znamená, že využijí veškerá strukturovaná data z veřejné správy, která máme k dispozici. Musíme pro to něco udělat, například doručit klientům uživatelský zážitek. Pokud se jim formulář skutečně předvyplní daty, je to zážitek a také vstřícný krok a občané zároveň mohou kontrolovat a opravovat správnost použitých dat a tím s veřejnou správou spolupracovat. Zapojme občany a podnikatele, ať nám pomohou vyčistit data, která má stát, budeme z toho profitovat všichni.

Zároveň je potřeba udělat analýzu svého datového fondu. Pokud nemáme fyzické zdroje na úřadě, měli bychom si je najmout. Dodavatelé systémů jsou takovouto analýzu schopni realizovat většinou v přijatelných termínech. Každý úřad, který disponuje nějakým formulářem (a to je každý úřad), by jej tedy měl zkontrolovat, převést do elektronické podoby a provést analýzu, zda skutečně potřebujeme všechny požadované údaje a zda jsou všechny formuláře nutné. Není to jednoduchá práce, ale pro zefektivnění veřejné správy nutná. Takovému přístupu by měl rozumět každý, kdo na konkrétním úřadě vykonává určitou agendu, protože totéž vlastně chce dnes po občanech v papírové verzi. Sbírá tato data a ví, proč. Udělat to elektronicky, je další logický krok. Mělo by se samozřejmě postupovat od priority nejčastější/nejvytíženější agendy. Možná k 1. 2. 2024 nebude hotovo 100 % agend, ale pokud by bylo zpracováno 80 %, byl by to skvělý výsledek. V současné situaci má ale Zdeněk Zajíček spíš obavu, že se nedostaneme ani přes 50 % úkonů, které by šlo elektronizovat.

PENÍZE, ALE KDE JE VZÍT?

Bylo by samozřejmě správné, abychom všichni měli v rozpočtech vyhrazeny dostatečné prostředky na výše popsané kroky. Je ale otázkou, zda jsme mysleli dopředu. Nyní jsme ve fázi, kdy se v rozpočtech spíše škrtá a je tedy velice pravděpodobné, že většině úřadů budou tyto klíčové prostředky spíše chybět. Zdeněk Zajíček se obává, že peníze na nějaký nový systém nejsou a nebudou, a tak jediná rozumná cesta podle jeho mínění je vzít to, co máme k dispozici, tedy digitalizovat papírové formuláře, získat strukturovaná data na vstupu, poslat je datovou schránkou a načíst je do vlastního systému. Samozřejmě můžeme vedle toho dále pracovat na lepším a efektivnějším modelu, ale toto je nejrychlejší cesta ke splnění zákona o právu na digitální službu. I proto vidí existenci datových schránek jako důležitou a velice oprávněnou.

Do „spuštění" zákona zbývá jen 513 dní (v den konání konference, tj. 5. 9. 2023). Musíme vzít to, co máme v kapacitách, jakými disponujeme, ale je to realizovatelné, smysluplné a vede k naplnění zákona.

Seyfor | Cloud and Security Competence Center

Implementace a adopce IT řešení, cloudových technologií a kybernetické bezpečnosti.

Jsme Seyfor – jedna z největších IT společností ve střední Evropě vyvíjející podnikové informační systémy pro podniky všech oborů a velikostí. Vedle toho nabízíme i širokou škálu dalších produktů, od zakázkových SW řešení přes datovou analytiku až po IT infrastrukturu. Součástí námi nabízených produktů a služeb je kompletní cyklus implementace nových technologií, od návrh řešení přes samotné nasazení až po adopční proces a zaškolení uživatelů.

Proč spolupracovat s námi?

- **Profesionalita:** Jsme tým certifikovaných expertů na dodávané technologie.
- **Odbornost:** Máme zkušenosti s velkými projekty v tuzemsku i zahraničí.
- **Týmový duch:** Pracujeme jako tým a zákazník je pro nás skutečným partnerem.
- **Důkladnost:** Nespokojíme se se standardem, vždy hledáme to nejlepší řešení.
- **Poctivost:** Zákazníci od nás mohou čekat rychlost, solidnost a nejvyšší kvalitu.

Co nabízíme?

- **Microsoft 365**

  Zajistíme všechny fáze procesu implementace technologií Microsoft 365, od přípravy až po zaučení zaměstnanců.

- **Microsoft Azure**

  Zajišťujeme kompletní infrastrukturu cloudové služby Azure, od vzdělání uživatelů přes migraci on-premise systémů až dodání softwaru a hardwaru.

- **Security**

  Nabízíme širokou škálu služeb majících za cíl maximální bezpečnost vašich dat. V oblasti kyberbezpečnosti jsou naše aktivity rozděleny do čtyř hlavních oblastí – Identifikace, Ochrana, Detekce a Reakce.

- **Adopční služby**

  Naše práce nekončí implementací a zaškolením. Adopční tým Seyforu pomůže vašim zaměstnancům skutečně pochopit největší přínosy nového řešení.

- **Profesionální služby**

  Proaktivní služby

  Zajišťujeme 24/7 poimplementační podporu, v jejímž rámci okamžitě reagujeme na varování systému a předcházíme haváriím. Zároveň pořádáme měsíční workshopy věnující se změnám a novým trendům v ICT, nabízíme pravidelné kontroly pro prevenci havárií, a spolupracujeme s vámi na plánech budoucnosti vaší ICT infrastruktury.

  Reaktivní služby

  Pružně reagujeme na incidenty a požadavky týkající se Azure a Office 365. U nejzávažnějších incidentů reagujeme nejpozději do dvou hodin, i u zásahů s nízkou prioritou se ale s vámi spojíme nejpozději do 12 hodin.

Jsme silní i tam, kde jiným síly docházejí.

Chcete podobné řešení?

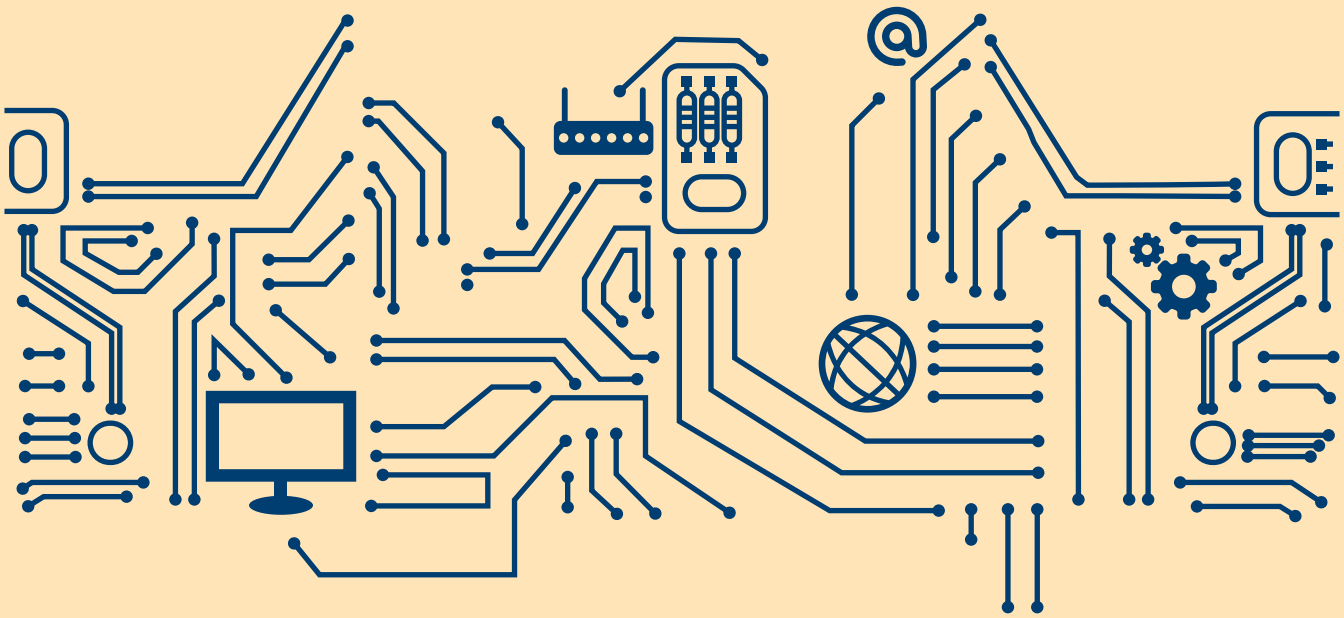
Karel Čapek | Account Manager
+420 606 764 132
karel.capek@seyfor.com

seyfor.com

Seyfor

Naše softwarová řešení naslouchají vašim problémům a skutečně je řeší

Just sey it!



DIGITÁLNÍ INFORMAČNÍ AGENTURA

První odborné vystoupení konference bylo v podání ředitele Digitální informační agentury Martina Mesršmída. Ten připomněl, že agentura fakticky nejen vznikla k 1. 4. 2023, ale už se konsolidovala a začíná fungovat tak, jak by úřad měl fungovat. DIA je tedy dle jeho slov schopna nejen vykonávat své zákonné povinnosti, ale rovněž „rozjíždět" nové projekty. Zároveň ale uvedl, že agenturu čeká velká změna organizační struktury k 1. 1. 2024. Definitivně by totiž měly být nově uspořádány delimitované útvary MV ČR a struktura bude poskládána podle aktuálních potřeb agentury. Nicméně zůstává v platnosti, že se DIA stará o vše, co převzala, tedy datové schránky, nebo Czech POINT, ale zároveň rozjíždí nové projekty. Upozornil, že ke konci roku proběhne velký redesign Portálu občana a aplikace GOV CZ. Zároveň bude předělán i vzhled NIA a přihlašování do Portálu občana. Věří, že uživatelský zážitek tak bude daleko lepší a odstraní se bariéry, které mohly doposud bránit využívání těchto služeb. Kromě toho pokračuje hodnocení schvalování projektů ICT v rámci odboru hlavního architekta a práce na otevřených a sdílených datech. Jednotlivým projektům se pak věnoval podrobněji

eDOKLADY

Probíhají intenzivní práce na aplikaci eDoklady, ale jak Martin Mesršmíd připustil, jedná se o lehce kontroverzní téma. Objevuje se totiž hodně otázek směřujících k tomu, zda národní aplikace eDoklady je potřeba v okamžiku, kdy se zároveň připravuje na evropské úrovni projekt eWallet. Tedy jestli by nebylo rozumné počkat na evropskou digitální peněženku a neplýtvat silami na národní obdobě. Je to samozřejmě téma pro diskuzi, ale DIA pracuje na eDokladovce a paralelně i na přípravě evropské digitální peněženky. Nedochází tedy k žádnému zpoždění. Martin Mesršmíd přitom věří, že evropská digitální peněženka bude tím, co nás dramaticky posune v digitalizaci dopředu, přičemž se bude jednat o silný nástroj jak pro ochranu osobní identity, tak i pro sdílení atributů, informací o konkrétní osobě, identitě, a to jak mezi veřejnou správou navzájem, tak i mezi VS a soukromým sektorem. Ale než k tomu dojde, tak si na projektu eDoklady můžeme vyzkoušet, jakým způsobem je možné do veřejné správy vpravit filozofii možnosti prezentovat se dokladem v elektronické podobě, který je úřad schopen číst a propojit si ho do svých vnitřních systémů. Zároveň je to cesta, jak naučit občany, co znamená vlastnit a používat identitní nástroj. Upozornil také, že mezi eDoklady a evropskou digitální peněženkou je značný rozdíl. Projekt eDoklady znamená pouze prezenční prokázání mé totožnosti (např. policii, na poště nebo jinému úřadu), tedy možnost elektronického dokladu, který předložíme pro fyzickou kontrolu. Evropská digitální peněženka bude primárně nástrojem elektronické identifikace, tzn. že bude orientována na identifikaci v on-line světě (na dálku).

Martin Mesršmíd uvedl, že je zajímavé sledovat, jak u eDokladovky probíhalo meziresortní připomínkové řízení. Zatím ještě nebyly vypořádány všechny připomínky, přičemž některé jsou poměrně zásadní. Většina z nich se týká finančních prostředků pro pořízení čtecích zařízení na jednotlivé úřady. Finančně analytický útvar MF má ale také připomínku k tomu, že by DIA měla být schopna vypořádávat přestupky, které vzniknou při zneužívání elektronických dokladů. Toho se ale DIA necítí být schopna, neboť nemá potřebné nástroje a neumí tak postihovat negativní chování. Diskuze k připomínkám tedy stále probíhá, ale i přesto bude vše připraveno tak, aby eDokladovka byla funkční. Zda a kdy se spustí, bude záležet pouze na tom, v jaké fázi bude legislativní proces.

Registr zastoupení

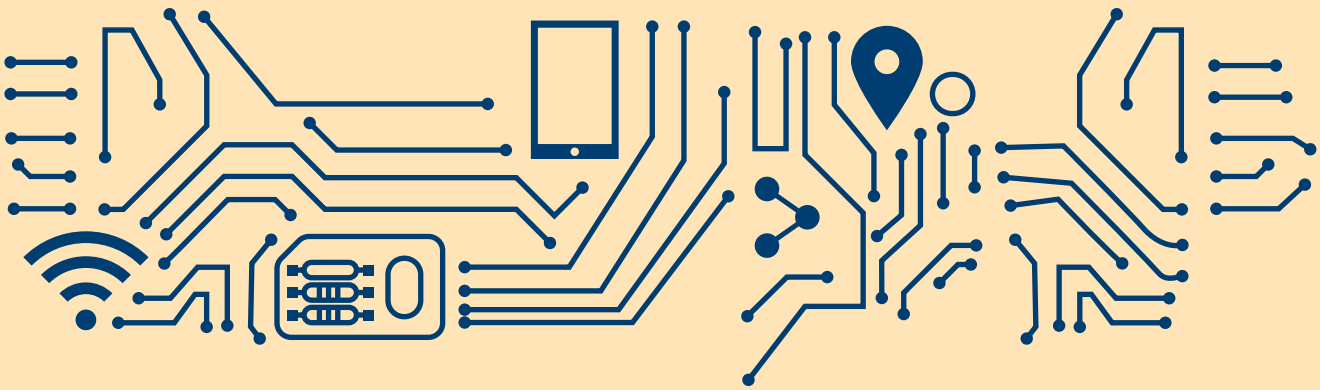
REZ je podle slov Martina Meršmída zajímavým projektem, který umožní každému občanovi někoho zastupovat při jednání s úřady, a to jednak na základě zákona (například své děti), ale také na základě pověření konkrétní osobou. Bude se jednat o centrální databázi, ve které budou uloženy tyto digitální mandáty. Důležité je, že celá databáze je k dispozici pouze pro on-line svět s cílem možného vyřízení digitálních agend z domova za konkrétní osobu. V první etapě bude k dispozici centrální část a DIA bude spolupracovat s Ministerstvem dopravy a Ministerstvem práce a sociálních věcí, následně pak Ministerstvem financí. V tomto centrálním řešení budou primárně uloženy mandáty ze zákona. Vedle toho budou existovat resortní části, kde budou uložena speciální oprávnění, která jsou pro daný resort specifická. První etapa by měla být hotova v polovině příštího roku, druhá, kdy již bude vlastní AIS registru zastoupení a budou napojena jednotlivá ministerstva, bude hotova v srpnu příštího roku. Třetí etapa bude pak postupným napojováním dalších úřadů na registr zastoupení. Ta bude realizována tak, jak kdo bude chtít a cítit se připravený k napojení. Důležitá je i informace, že toto napojení je dobrovolnou záležitostí, nejedná se tedy o něco, co by bylo vyžadováno.

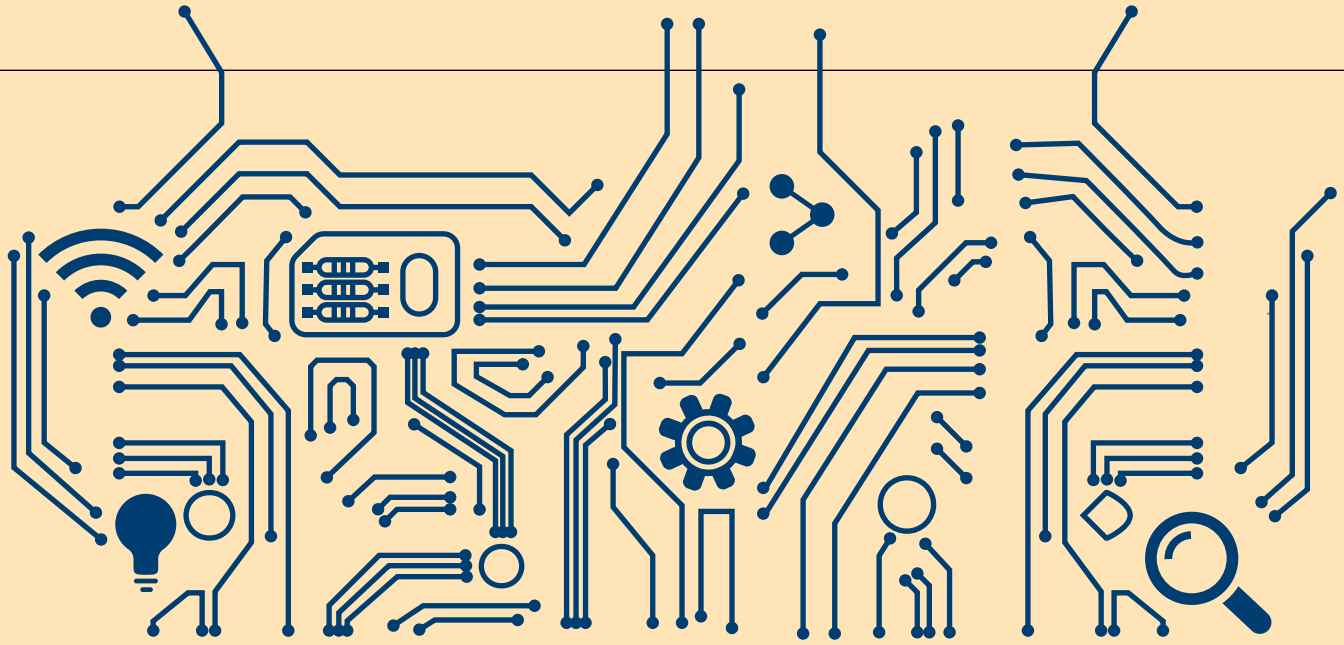
Kompetenční centra

Fakticky už nic takového není, je to terminus technicus, který se zažil a používá i nadále. Jedná se o nový tým lidí, které chce DIA financovat z Národního plánu obnovy. Nyní je zpracován projekt, který už prošel schvalovacím procesem, a podle předpokladu by DIA mohla ke konci roku začít nabírat odborníky do „kompetenčních center". Tito odborníci by měli být vysíláni na jednotlivé úřady, aby tam zmapovali a popsali datové zdroje a informační potřeby daného úřadu tak, aby tyto instituce byly schopny vystavit datové zdroje na informační systém sdílené služby. Martin Meršmíd věří, že tento krok dokáže zrychlit digitalizaci, neboť se jedná o pomoc úřadům, které často nemají dostatek odborníků. Problémem je ovšem skutečnost, že Ministerstvo financí plošně nastavilo limit pro platy u projektů Ministerstva průmyslu a obchodu. Momentálně tedy DIA řeší otázku, zda za takových okolností bude mít tento projekt smysl, neboť toto platové omezení bude rozhodně komplikovat nábor skutečných odborníků.

EGC kalkulátor

Martin Meršmíd vyzdvihl rovněž projekt EGC kalkulátor. Jedná se o nástroj, se kterým aktuálně pracuje odbor hlavního architekta při schvalování projektů. Vznikl jako dobrý příklad spolupráce státního a soukromého sektoru, konkrétně OHA, IBM a ICT Unie. Jeho účelem je vyčíslit náklady a srovnat různé varianty řešení informačních systémů. Celému projektu byla věnována samostatná prezentace v odpoledním bloku e-government (najdete na str. 38).





Zákon o právu na digitální služby

V této souvislosti byla sestavena pracovní skupina ze zástupců mnoha úřadů, která se zabývá interpretací zákona a konkrétními praktickými postupy, jak zákon naplnit a jak nesklouznout ke zkratkovitým řešením, které by nenaplňovaly podstatu digitalizace. Cílem je, aby v červenci 2024 bylo 90 % služeb veřejné správy digitalizováno. Momentálně je to přání, ale Martin Mesršmíd věří, že se tomuto číslu přiblížíme.

Datové schránky

Přibylo více než 2 mil. nových „datovek“, což znamená, že celkem jich byly zřízeny již 4 miliony a nárůst stále pokračuje. Je potěšitelné, že se tak děje nejen ze zákona, ale rovněž na vyžádání. Čeká nás tedy především zvýšení kapacit datové správy, ke kterému dojde souběžně s již zmiňovanými úpravami Portálu občana. Protože řada uživatelů má výhrady ke krátké době uložení v DS (90 dní), bude nově v rámci Portálu občana možné ukládat data neomezeně dlouho. DIA rovněž eviduje stížnosti na počet DS, respektive nekomfortní přechod z jedné do druhé DS, pokud je osoba vlastníkem většího počtu DS. I to by měla řešit plánovaná úprava PO. V jeho rámci by měl být přechod (přepínání) mezi jednotlivými datovými schránkami jednoho vlastníka natolik optimalizováno, že bude uživatelsky příjemné a pohodlné.

Czech POINT

Služba Czech POINT funguje podle Martina Mesršmída dobře bez nějakých zásadních výhrad a problémů. Jedná se o „páteř“ e-governmentu a je určena především těm, kteří se nechtějí nebo z nějakých důvodů nemohou připojovat on-line. V rámci Czech POINTu se nyní „rozjíždí“ e-legalizace, tedy elektronická legalizace papírových dokumentů - pilotní provoz bude od 1. 10. 2023. Nejvíce využívanou službou v rámci CZP je autorizovaná konverze na žádost uživatelů.

Hodnocení projektů

Odbor hlavního architekta (OHA) plní svoji úlohu tak, jak bylo nastaveno již dříve na MV ČR, nicméně jeho snahou je při zachování toho dobrého rozšířit jeho působnost a schválit více projektů, tj. celý proces pokud možno škálovat a urychlit, protože zatím je vnímán spíše jako určitá bariéra. Cílem je tedy, aby se jednalo spíše o pomocný/podpůrný a hlavně plynulý proces.

Převod ROBu a ROSu

Aktuálně je registr obyvatel ve správě MV ČR a registr osob ve správě ČSÚ. DIA pracuje na tom, aby byly k říjnu 2024 převedeny pod agenturu, tedy jejich věcná správa, neboť technická správa už převedena je.

Závěrem Martin Mesršmíd upozornil, že základní registry (ROB, ROS a RPP) běží stále na starém hardware. S jeho obměnou bylo započato v loňském roce. Letos se úspěšně podařilo vysoutěžit nový HW a byly podepsány smlouvy na dodávku tak, aby se nové vybavení implementovalo na přelomu roku. Každopádně cílem DIA je, podle slov jejího ředitele, stát se silným úřadem, který bude schopen pomáhat všem ostatním institucím. Z tohoto pohledu považuje za zásadní postavit „kompetenční centra“ a vysílat již zmíněné odborníky a urychlit tak digitalizaci.

Následnou diskuzi a odpovědi Martina Mesršmída na otázky diváků stejně jako videozáznam jeho prezentace naleznete na www.egovernment.cz v sekci MIKULOV23.

PRACUJEME NA DIGITÁLNÍ TRANSFORMACI ČESKA

ICZ - špičková IT řešení od špiček v oboru

[ZDRAVOTNICTVÍ]

[VEŘEJNÁ SPRÁVA]

[INFRASTRUKTURA]

[ŘÍZENÍ LETOVÉHO PROVOZU]

[OBRANA]

[BANKOVNICTVÍ A POJIŠŤOVNICTVÍ]

[BEZPEČNOST]

[LOGISTIKA]

[ŘÍZENÍ LETOVÉHO PROVOZU]

www.iczgroup.com

eDoklady nebo eWallet?

O tématu evropské elektronické peněženky se ve svém vystoupení již zmiňoval Martin Mesršmíd. K rozsáhlejší diskuzi o tomto evropském projektu i o národním projektu eDoklady jsme si kromě ředitele Digitální informační agentury přizvali ještě za bankovní sektor Pavla Koláře z ČSOB a za certifikační autority Petra Budiše, generálního ředitele a předsedu představenstva I.CA.

Bavili jsme se o projektu, který vychází z požadavku EU a kterému říkáme evropská elektronická peněženka (eWallet), s níž bychom se měli v běžném životě potkat v roce 2026, a o českém národním projektu eDoklady, jehož výsledek, pokud se vše podaří, bychom měli používat již příští rok. V debatě pánové připustili, že množství elektronických peněženek, kterými se to v současné době jen hemží, znamená určitý zmatek, ale tak tomu v minulosti bývalo při vývoji a „stabilizaci" zásadních oblastí elektronizace (například množství internetových prohlížečů, e-mailových klientů atp.).

Evropská elektronická peněženka (eWallet)

Na eWallet bychom měli v současné chvíli nahlížet jako na oblast, ve které bude mezi dodavateli možných řešení probíhat velká soutěž. Zcela jistě tak může spontánně vzniknout celá řada variant, které budou kompatibilní a přitom budou nabízet určité odlišnosti. Tedy bude pestrý výběr a to není na škodu. Současný stav je do jisté míry zmatený také kvůli velkému počtu identitních prostředků, které fungují na různé úrovni zabezpečení a na různém principu. V oblasti eWallet naproti tomu směřujeme ke stavu, kdy sice bude více e-peněženek, ale fungujících na stejném principu. Kromě elektronických peněženek budou stále existovat i jiné identitní prostředky, které samozřejmě s příchodem projektu elektronické peněženky nezanikají, ale je velice pravděpodobné, že evropská elektronická peněženka bude získávat dominanci, neboť bude nabízet uživatelům větší užitek než ostatní nástroje, které jsou jednoúčelové.

Slovo peněženka je v tomto směru poněkud zavádějící. Evropská digitální peněženka není totiž určena k realizaci plateb, i když i o nich se do budoucna trochu uvažuje. Primárně se jedná o nástroj identitní, tedy určený k prokázání toho, kdo jsem, včetně dalších atributů týkajících se mé osoby (úrovně vzdělání, různých získaných oprávnění, jako je řidičský průkaz, zbrojní průkaz, ale například i potvrzení o bezdlužnosti atp.). Na základě vlastního uvážení mohu tyto údaje elektronickou cestou konkrétnímu subjektu prokázat.

Princip je tedy stejný jako v reálném světě. Elektronická peněženka je skutečně peněženka, ve které nosím doklady. Ta „fyzická" peněženka může být z různého materiálu a od různých výrobců, ale uvnitř mám konkrétní doklady určité vypovídající hodnoty. Totéž platí pro elektronickou evropskou peněženku s tím rozdílem, že zde mohu mít veškeré doklady, které člověk v běžných životních situacích potřebuje mít, tedy patrně daleko větší množství, než které obvykle nosíme v té neelektronické. Evropskou se tato peněženka nazývá, protože bude minimálně v Evropě plně použitelná kdekoliv. Vize je taková, že s tímto nástrojem, který bude integrován zpravidla do mobilního zařízení, budu moci cestovat po světě a nebudu potřebovat nic jiného. Tato fáze je v současnosti ještě trochu vzdálená, neboť nebude patrně praktické hned od počátku cestovat jen s elektronickou verzí. Alespoň ty základní doklady zřejmě „pro jistotu" budeme po nějakou dobu vozit duplicitně. Nicméně cílem je situace, kdy skutečně v rámci kontinentu budeme moci získat například ubytování, půjčit si auto atp. kdekoliv pouze při předložení evropské elektronické peněženky, respektive konkrétního dokladu, který je v ní uložen. Uživatelský komfort a rozšíření jsou tedy v tomto směru velice žádoucí, ale zároveň je nutno dbát na vysokou míru bezpečnosti. Ta je tím nejdůležitějším aspektem projektu, protože selhání a ztráta důvěry by byl jeho konec.

Jednou z podstat elektronické peněženky by měla být spolupráce soukromého a veřejného sektoru, podobně jako tomu bylo v případě bankovní identity. Bankovní identita je projektem, který byl dostatečně diskutován, stála za ním skupina poslanců, která jej prezentovala kolegům a ve sněmovně byl příslušný zákon přijat naprostou většinou. Účinnosti nabyl 1. 1. 2021 a nyní je vydáno pře 5 mil. identit a 1,3 mil. je unikátních uživatelů. Panuje tedy přesvědčení, že podobně by měl bankovní sektor spolupracovat se státem i na rozvoji elektronické digitální peněženky. Je ovšem nutné, aby byla zřetelná smysluplnost tohoto projektu. Neměl by být například orientován pouze na veřejnou správu. Běžný občan komunikuje s veřejnou správou ve skutečnosti zřídka, víceméně jednorázově. Daleko častěji se obrací na soukromý sektor (banky, operátory, dodavatele energií...), a proto by bylo vhodné, aby prostřednictví elektronických dokladů bylo možné prokazovat svoji identitu i tímto směrem.

eDOKLADY

Projekt eDoklady je podobný evropské peněžence, ale je výrazně jednodušší. Jedná se totiž pouze o prezenční prokázání mé totožnosti, tedy elektronický doklad, který předložíme pro fyzickou kontrolu pomocí čtecího zařízení. Ale s tím, kdo mě kontroluje, jsem v přímém kontaktu. Evropská digitální peněženka bude primárně nástrojem elektronické identifikace, tzn. že bude orientována na identifikaci v on-line světě, tedy na dálku. Podstatné je, že se vždy jedná o zásadní změnu prokazování a vůbec chápání identity a elektronického podpisu. To nejtěžší, co zabere nejvíc času, bude naučit dotčené subjekty (OVM) pracovat s novými nástroji a novým způsobem. Proto je dobré, že projektu evropské elektronické peněženky bude předcházet „pilot" v podobě národního projektu eDoklady. Je sice o něco jednodušší, ale vychází z obdobného principu, a hlavně má stejné zúčastněné strany, což by mohlo napomoci implementaci principu do našeho úřadování.

Termíny

Český projekt eDoklady by měl být funkční v lednu příštího roku. Otázkou je, zda se bude stíhat legislativní proces, ale předpoklad náběhu účinnosti zákona je takový, že ústřední správní úřady by měly akceptovat prokázání identity prostřednictvím eDokladu již od 1. 1. 2024. Další úřady budou mít termín od 1. 7. 2024 a ke konci roku tato povinnost padne i na zastupitelské úřady. U evropské digitální peněženky předpokládáme, že rok 2026 by měl být rokem, kdy se bude zavádět do života. Je nutno dopracovat ještě řadu detailů, následně budou zpracovány prováděcí dokumenty a teprve pak nastane dvouleté období, kdy má každý stát čas implementovat.

A zpoždění

Vzhledem k tomu, že se ještě nepodařilo vypořádat celé připomínkové řízení, není pravděpodobné, že by Poslanecká sněmovna Parlamentu stačila zákon ještě v říjnu projednat a například v listopadu jej schválil Senát. Bude zde tedy určitě časový skluz, který se dá využít k tomu, aby se odladilo co nejvíce legislativních i technologických uzlových bodů. V současnosti se například vášnivě diskutuje o variantách povinné či dobrovolné účasti pro soukromé subjekty atp. Nicméně je to pochopitelné, neboť se jedná skutečně o revoluční změnu, a to nejen v rámci veřejné právy.

PÁNOVÉ ROVNĚŽ ODPOVÍDALI NA KONKRÉTNÍ DOTAZY NAŠICH ÚČASTNÍKŮ:

- **Je rozumné realizovat českou verzi, když za pár let přijde evropská?**

  Jak bylo řečeno, ti, kteří budou s elektronickým prokazováním identity pracovat, budou v obou případech, tedy „národní" i „evropské" peněženky stejní. Evropskou peněženku není možné realizovat v nějakém předstihu. Dá se to tedy chápat i tak, že eDoklady jsou vlastně jakousi „light" verzí, díky které si můžeme zvyknout a být tak připraveni na evropský model.

- **Musím mít doklady „nahrané" v mobilu, nebylo by možné ověřování v základních registrech?**

  Samotný princip je takový, že údaje by měly být prokazatelné on-line i off-line. Občan – vlastník dat - může korigovat, jak široké spektrum informací má být prokazováno, respektive které a v jakém rozsahu. Kdyby se kvůli tomu pokaždé musel připojovat na data v základních registrech, bylo by to zdlouhavější. Takto se předpokládá rychlý kontakt mezi čtecím zařízením a elektronickou peněženkou. Je nutno pamatovat, že uvažujeme i o prokazování identity například subjektům ze soukromého sektoru, které nemají přístup k ověření v základních registrech. Ale pro určité případy, které potřebují „hlubší" ověření, je samozřejmě možné připojení na základní registry.

- **Není možné, aby se jednalo o jednoduchý scan dokladů?**

  To rozhodně není možné. Vždy by se mělo jednat o challenge response, tedy že já budu digitální cestou vyzván k předložení konkrétního průkazu. Cesta bude sestavená kryptograficky tak, aby bylo jasné, které strany spolu komunikují, a následně v offline režimu, třeba přes Bluetooth nebo přes QR code, tato komunikace proběhne. Je to důležité z pohledu bezpečnosti. Dokonce platí, že i ověřující strana ode mě, jako od vlastníka toho datového zdroje, musí dostat povolení, což znamená, že mohu zpřístupnit jen určité vybrané informace.

- **Jak to je s financováním?**

  Snažíme se přesvědčit politickou reprezentaci (vládní i opoziční) o tom, že by tento projekt měl být vystavěn na spolupráci státu a soukromého sektoru. Mluvíme o potřebě velkých finančních zdrojů a zapojení soukromého sektoru je důležité nejen s ohledem na know-how, ale i jeho motivaci k návratnosti investic. Stát by si měl držet regulační (bezpečnostní a správní roli), na druhé straně realizace a marketing by mohly být na straně komerčních subjektů. O tom diskutuje pracovní skupina pod RVIS, která bude toto řešit. Diskutovaly se různé modely, ale v zásadě se bavíme o trojúhelníku: užitek pro občana, zisk pro firmy a bezpečnost pro stát. A první dva body umožňují firmám najít nové obchodní modely s tím, že se mohou odblokovat některé transakce závislé na důvěře. Pak by mělo být možné například poskytovat slevy, věrnostní programy, půjčky atp. Určitě se v této souvislosti objeví nové obchodní modely, z nichž budou mít benefit všichni zúčastnění.

- **Kolik zaplatí úřad za vybavení**

  U evropské elektronické peněženky ještě nevíme, to je příliš vzdálené. Vybavení v rámci projektu eDoklady je rovněž předmětem meziresortních jednání. Minimálně ústřední správní úřady si budou toto muset „narozpočtovat", aby se mohly vybavit. Důležité ale je, že zvolený protokol eliminuje nutnost fyzických čteček. Mohou být použity mobilní telefony, speciální čtečky, ale právě i on-line protokol (QR code, který si uživatel načte a on-line se propojí s backendem systému úřadu). Platí tedy, že v případě projektu eDoklady bude muset vybavení financovat stát, na druhé straně soukromé subjekty si to budou muset platit samy. Odhad pouze České bankovní asociace hovoří o tom, že implementace, změna procesů, přizpůsobení datových úložišť a zaškolení personálu v tomto segmentu vychází na 410 mil. korun během dvou let. I proto je jedním z diskutovaných požadavků dobrovolné, nikoli povinné zapojení soukromých subjektů do projektu eDoklady.

Na závěr diskuze jsme pány požádali o odhad, kdy se domnívají, že se budeme v ČR prokazovat elektronickými doklady v rámci projektu eDoklady?

Ředitel digitální informační agentury Martin Mesršmíd je optimistický a domnívá se, že se tak skutečně stane počátkem příštího roku. Možná ne 1. 1. 2024, ale rozhodně začátkem roku. Připouští ale, že jeho optimismus může být zkreslen tím, že nevidí do zákonitostí legislativního procesu.

Pavel Kolář z ČSOB připouští, že se tak stane někdy v příštím roce, ale nemyslí si, že na jeho začátku. Počátek roku by viděl jako testovací proces, ale skutečná akceptace bude možná až v průběhu roku.


ZAČNĚTE
ŽÍT PRÉMIOVĚ
ČSOB
Premium
Zasloužíte si nadstandardní služby
doma i na cestách.
Sjednejte si Premium Konto
jednoduše v mobilu.
Z bankomatů vybíráte po celém světě zdarma,
získáte exkluzivní pojištění a další výhody.
www.csobpremium.cz | Premium linka 800 370 370

Evropská peněženka digitální identity a atributová autorita

Španělské předsednictví Rady Evropy si jako jeden ze stěžejních cílů vytyčilo přijetí revidovaného nařízení eIDAS, často uváděného pod zkratkou eIDAS2, jež má těžiště v evropských peněženkách digitální identity, resp. European Digital Identity Wallet, často uváděný pod zkratkou „EUDI Wallet" nebo „EUDIW".

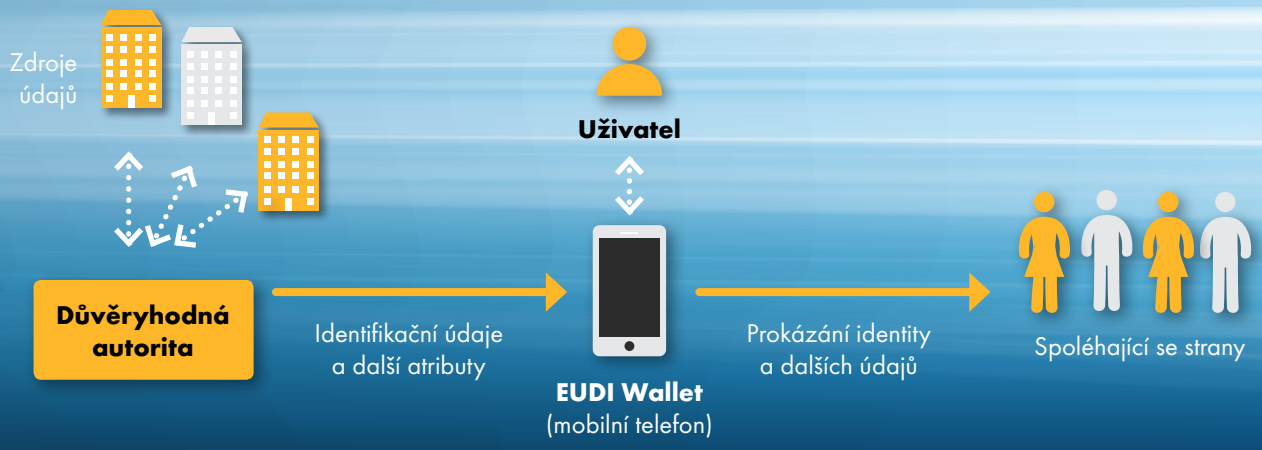
Dalo by se říci, že především z důvodu jeho zavedení byl Evropskou komisí (EK) návrh zpracován a vyslán do legislativního procesu. V jedné z četných charakteristik EK uvádí, že: „peněženka EUDI radikálně změní způsob, jakým se mohou občané a podniky digitálně identifikovat při přístupu k veřejným a soukromým službám v celé Evropě a používat svůj chytrý telefon bezpečným a pohodlným způsobem. Občané tak budou moci kontrolovat své osobní údaje uložené v peněžence. Peněženka bude rovněž vybavena mechanismy pro minimalizaci sdílených dat pro přístup ke službám."

Má se jednat o nový způsob prokazování totožnosti a dalších údajů, například o vzdělání, profesní kvalifikaci či o různých zmocněních a právech. Peněženky by měly být v řadě aspektů plnohodnotnou alternativou k fyzickým dokladům. Půjde jimi řešit řadu životních situací nejen vůči úřadům, ale i vůči soukromému sektoru. Důležité je, že peněženky by měly mít formu mobilní aplikace a sám uživatel by mohl rozhodovat, jaké údaje konkrétnímu subjektu poskytne. Díky peněžence bude možné také vytvářet kvalifikovaný elektronický podpis. A kdy se EUDIW dočkáme? Prozatím se navrhuje, aby se tak stalo 24 měsíců po přijetí prováděcích aktů, které mají být vydány do 6 měsíců po přijetí eIDAS2. Obavy, že se občan EU neobejde bez chytrého telefonu, jsou liché, stávající způsoby prokazování a identifikace zůstanou zachovány.

Proč je nutný předpis EU, když určité formy peněženek jsou dostupné už dnes? Především je nutný legislativní rámec na úrovni EU a společné řešení vysoké míry bezpečnosti a ochrany osobních údajů. To vše, aby peněženky mohly být uznávány přeshraničně. EUDIW by měly vydávat orgány členských států, nebo jimi pověřené subjekty. Pro plnění své funkce nemohou EUDIW existovat izolovaně, proto se hovoří o celém ekosystému EUDIW.

A co vše bychom měli mít možnost pomocí EUDIW prokázat? Kromě totožnosti a řidičského průkazu, samozřejmě i věku (při nákupu alkoholu i při založení účtu na sociálních sítích), vzdělání a získané kvalifikaci bude možné použití v e-preskripci pro možnost využívat lékárny v EU, bankovní služby, a to jak při otevření účtu, tak při platbách díky možnosti ukládat přihlašovací údaje. Při cestování např. pomůže urychlit nástup do letadla a překročení hranic (např. uložením digitálních cestovních přihlašovacích údajů). Lze ji využít k usnadnění volného pohybu např. uložením Evropského průkazu zdravotního pojištění. Přístup ke komerčním službám by měl být uplatňován zejména v případě požadavku silného ověření, v „citlivých" oblastech pak povinně. Přístup ke službám státu a možnost vytvářet kvalifikovaný elektronický podpis jsou už uvedeny výše.

Jednoduché schéma ekosystému EUDIW je možné znázornit následovně:



Jedním ze základních stavebních kamenů celého ekosystému EUDIW je kromě vlastní aplikace EUDIW a zdrojů autentických dat i nezbytný mezičlánek, jehož úkolem je zprostředkovat komunikaci mezi celoevropsky jednotným rozhraním aplikace EUDIW a příslušnými proprietárními systémy v jednotlivých členských státech, využívanými jako autentické zdroje dat, u nás to jsou např. základní registry. Zprostředkovatelskou funkci by měli zastávat poskytovatelé kvalifikovaných služeb elektronického potvrzování atributů, zkráceně atributové autority (AA, resp. QEAA).

Ve srovnání s klasickými elektronickými certifikáty pro autentizaci a/nebo podpisy mají atributová potvrzení podobné vlastnosti, ale jiný formát a jinak se ověřuje jejich platnost atd., mají však i mnoho shodných vlastností. Na druhé straně jsou na jejich vydavatele kladeny v zásadě stejně přísné bezpečnostní požadavky, jejichž cílem je zajistit, aby systém jako celek mohl uživateli a spoléhajícím se stranám poskytnout vysoký stupeň důvěry pro data, jimi (byť zprostředkovaně) poskytovaná. I proto řeší návrh revize nařízení eIDAS otázku zajištění důsledného prosazování požadavků na zabezpečení systémů pro elektronickou identifikaci obdobně jako v případě požadavků na poskytovatele služeb vytvářejících důvěru – tj. celého systému akreditací, periodicky prováděných auditů a kontroly státem určenými dohledovými orgány.

Pro zavedení EUDIW v podmínkách České republiky bude zajisté nejen nutné, ale především přínosné zapojení komerčního sektoru, specificky bankovních institucí, které mohou zprostředkovat využívání peněženky širokému okruhu svých klientů. Stát poskytne ověřené datové zdroje a prostředí pro poskytovatele kvalifikovaných služeb elektronického potvrzování atributů. Evropská peněženka tak poskytne možnost sdružit v mobilním zařízení takové údaje, které uživatel výslovně potvrdí a v každodenním životě používá. Jedině každodenní používání povede k rozvoji dalších funkcí peněženky přínosných pro jejího držitele.

Ing. Petr Budiš, Ph.D., MBA
generální ředitel
První certifikační autorita, a.s.

SASE: zajištění kyberbezpečnosti ve světě cloudu a hybridní práce

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

Co je SASE

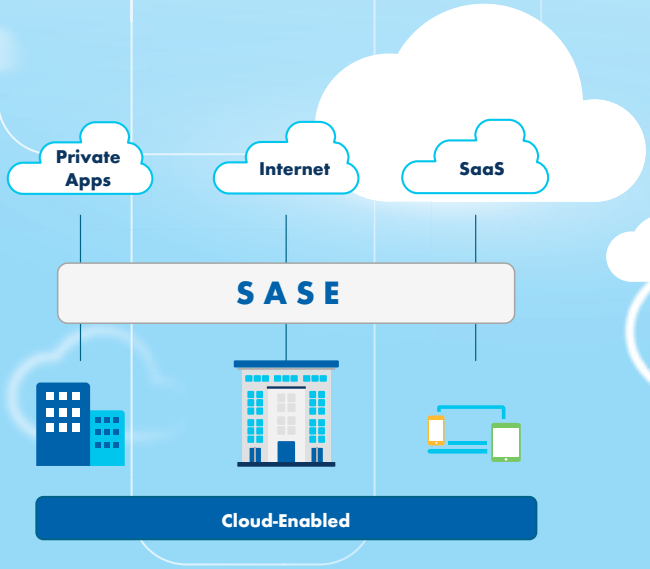
SASE poskytuje bezpečné a bezproblémové připojení k jakékoli aplikaci, přes jakoukoli síť, z jakéhokoli místa nebo zařízení. V prostředí SASE se integrují síťové a bezpečnostní funkce do jednotného cloudového řešení nebo služby. Na rozdíl od tradičních bezpečnostních řešení posouvá bezpečnostní politiky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

Sítě a bezpečnost v souladu

SASE znamená přechod z aplikačního modelu zaměřeného na datová centra (DC Centric modelu) na model s podporou internetu a cloudu (Cloud-enabled). Od IT týmů vyžaduje adopce principů SASE zcela přehodnotit síťovou strategii. Zároveň jim ale pomáhá zajistit bezpečné a bezproblémové prostředí i pro uživatele a aplikace mimo infrastrukturu organizace, kde jsou s vyšší pravděpodobností vystaveni náhodným nebo záměrným bezpečnostním útokům. To má v systémech veřejných institucí, které často pracují s citlivými osobními údaji, mimořádný význam.

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

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



Nic nového pod sluncem?

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

Tak to ale není, protože nasazení SASE přináší dvě změny:

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

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

Integrované řešení jednoho dodavatele

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

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

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

Hlavní výhody Cisco SASE

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

Další informace související s Cisco SASE lze najít například zde: https://www.cisco.com/site/us/en/solutions/secure-access-service-edge-sase/index.html

Milan Habrcetl,
Cisco Cyber Security Specialist

Bitdefender

FERRARI
TEAM
PARTNER

Získejte licence pro POC na 2 měsíce zdarma

+ navíc **30% sleva** na všechny XDR sondy

Subjektům státní správy a **samosprávy** nabízíme Licence pro POC na 2 měsíce zdarma a slevu 30 % na všechny XDR sondy k hlavnímu řešení Bitdefender. Akce platí do 31.12.2023.

Bitdefender podporuje společnost Ferrari pokročilou analýzou hrozeb, která zlepšuje detekci a reakci na kybernetické hrozby.

Otestujte si technologii, na kterou sází nejen Ferarri.
Bitdefender chrání více jak 600 Miliónů zařízení po celém světě. Přidejte se k nám.

Trusted. Always.

Rezervujte si
konzultaci zdarma

Zájem o penetrační testy poroste, očekává se větší zájem státní správy

V rychle se vyvíjejícím prostředí kybernetické bezpečnosti hledají organizace neustále způsoby, jak zajistit bezpečnost a odolnost své infrastruktury. Jedním z kritických aspektů tohoto bezpečnostního prostředí je penetrační testování, proaktivní přístup k posuzování schopnosti organizace odolávat kybernetickým hrozbám. Expert společnosti Eviden Tomáš Hlavsa upozorňuje, že zájem o tyto testy dramaticky naroste jak mezi firmami, tak mezi subjekty veřejné správy. Těm ale budou velmi pravděpodobně chybět odborníci na kyberbezpečnost – nejen pro testování bezpečnosti systémů, ale i pro běžný provoz vlastního Security Operations Centra (SOC).

Práce penetračních testerů je dalece vzdálená romantice dobrodružných filmů. Ale pro bezpečnost organizace je extrémně důležitá.

„Celkový počet subjektů podléhajících stávajícímu zákonu o kybernetické bezpečnosti je nyní ve vyšších stovkách. Avšak s nástupem směrnice NIS2 očekáváme řekněme patnáctinásobný nárůst tohoto čísla. Penetrační testy jsou jedním ze základních nástrojů, jak ověřit, že máte správně nastavenou kyberbezpečnost a že jsou systémy, aplikace, data i zařízení chráněna tak, jak mají být. Představitelé veřejné správy mají zodpovědnost nejen za bezpečnost vlastní organizace, ale zodpovídají také za zřizované organizace – na úrovni obce, kraje i celého státu. Předpokládám, že poptávka po penetračních testech se zvýší zhruba desetkrát," říká Tomáš Hlavsa, bezpečnostní ředitel společnosti Eviden.

Každodenní zajištění bezpečnosti – vlastní SOC je pro většinu organizací luxusem

Podívejme se nejprve na to, jakým způsobem mohou organizace veřejné správy zajistit pravidelný, každodenní dohled nad bezpečností vlastní IT infrastruktury. Běžně takový dohled zajišťuje bezpečnostní centrum SOC (Security Operations Center). Klíčovou otázkou pro organizace ale je, zda ho budovat a provozovat vlastními silami, nebo některý z těchto úkolů přenechat externím odborníkům.

„Nejnáročnější cestou je budování vlastního SOC. Jako Eviden s tím máme řadu zkušeností napříč Evropou a jsme schopni s tím zákazníkům pomoci. Jednodušší cestou je ale pro mnoho organizací využití cloudového SOC jako služby, nebo propojení jejich organizace na nově budované vládní dohledové centrum – VDC. Jeho možnosti na konferenci v Mikulově prezentoval pan ředitel Rohel z NAKITu a pro většinu organizací veřejné správy to je optimální cesta, jak zajistit vlastní kyberbezpečnost," říká Tomáš Hlavsa.

Poznamenává ale, že ani napojení – onboarding – do VDC není triviální záležitostí. *„Je to časově náročný proces, který trvá 2 až 6 měsíců, a jakákoliv komplikace ho prodlouží – například chybějící dokumentace dodavatelů, či nedostatečná součinnost. Vždy nejprve zpracujeme studii proveditelnosti a naši experti provedou vaši organizaci celým procesem. Mechanismy, které máte v organizaci zavedeny, je třeba doladit, zpřísnit a přizpůsobit novým předpisům a legislativě,"* vysvětluje Tomáš Hlavsa.

Penetrační testování odhalí, jestli vaše bezpečnostní řešení obstojí v realitě

Penetrační testování je metoda hodnocení schopnosti organizace odolávat kybernetickým hrozbám. Hodnotí odolnost, zabezpečení a zranitelnost organizace. Cílem penetračního testování je identifikovat zranitelná místa v infrastruktuře a systémech organizace a posoudit jejich náchylnost ke zneužití. Zranitelnosti lze definovat jako softwarové chyby, které umožňují neoprávněné akce. Otevírají dveře různým typům útoků, včetně odepření služby, kompromitace identity, narušení služeb nebo vzdáleného převzetí. Některé zranitelnosti jsou dokonce neznámé a označují se jako „zranitelnosti nultého dne". Ty jsou kritické, neboť proti nim neexistuje žádná obrana a jsou útočníky zneužívány, aniž by o tom měla organizace sebemenší tušení. S těmito zranitelnostmi lze na dark webu obchodovat za značné částky, od tisíce až po statisíce dolarů. Vzhledem k neustále se vyvíjejícímu digitálnímu prostředí zůstane penetrační testování pro organizace kritickým postupem při ochraně jejich citlivých dat a digitálních aktiv. Etičtí hackeři neboli pentesteři se budou i nadále pohybovat ve složitém terénu legality, etiky a bezpečnosti, aby poskytovali cenné poznatky o kyberbezpečné připravenosti organizace.

„Penetrační testování není pouhou službou; je to proaktivní obranný mechanismus, který organizacím umožňuje identifikovat a řešit zranitelnosti dříve, než je mohou záškodníci zneužít. Díky specializovanému týmu odborníků společnosti Eviden mohou organizace udržet náskok před kybernetickými hrozbami a pokračovat v inovacích digitálního věku," říká Tomáš Hlavsa.

Mít vlastní tým pro penetrační testování je vzácnost, expertů je málo

Řada běžných IT dodavatelů nemá k dispozici vlastní tým pro penetrační testování, protože jeho udržování je velmi náročné – z hlediska organizace, kontinuálního vzdělávání, vysoké motivovanosti a s tím souvisejícími náklady. Společnost Eviden řeší tento problém diverzifikací svého týmu v pěti evropských zemích, který zahrnuje více než 300 odborníků v Polsku, Rumunsku, České republice, Rakousku a Německu. Tato síť spolupracujících odborníků umožňuje společnosti Eviden efektivně nasazovat zdroje k řešení různých výzev v oblasti kybernetické bezpečnosti v celé Evropě.

„Komerční firmy dávno využívají penetrační testování, aby si ověřily praktické zabezpečení svých systémů. S ohledem na NIS2 s tím budou muset začít i organizace veřejné správy," říká Tomáš Hlavsa, vedoucí oddělení Big Data & Security a bezpečnostní ředitel společnosti Eviden.

Tomáš Hlavsa hrdě poznamenává, že Eviden se může pochlubit jedním z největších týmů penetračních testerů v Evropě. Zdůrazňuje, že je prakticky nemožné udržovat malý tým například 50 osob a využívat je sporadicky. Poptávka po službách penetračního testování kolísá a existence rozsáhlého a různorodého týmu zajišťuje flexibilitu a pružnost v reakci na tyto dynamické potřeby.

Nevěřte nabídkám s nejnižší cenou, práce profesionálních pentesterů je drahá

„Kvalitních dodavatelů penetračního testování je velice málo. Některé firmy sice nabízejí levné služby, ale skutečná odbornost vyžaduje větší tým s kvalifikací a zkušenostmi, což je v České republice vzácné. To není způsobeno nedostatkem ochoty, ale spíše nedostatkem kvalifikovaných pracovníků," říká Hlavsa.

Kvalita penetračních testů závisí na jejich rozsahu a může být nákladnější, přičemž cena testování webových aplikací se obvykle pohybuje kolem 12 000 Kč za manday. Při testování zaměřeném na zabezpečení vnitřní infrastruktury organizace, e-mailového systému, dat nebo konkrétních aplikací bývá cena vyšší, protože tyto služby vyžadují vyšší odbornost.

„Při vyhledávání služeb penetračního testování nebo etického hackingu je nezbytné jasně definovat své cíle a specifikovat úkol. Kvalitní testování začíná dobře definovaným zadáním v rámci organizace. A určitě se při něm nelze zaměřit na nejnižší nabídkovou cenu jako hlavní kritérium," uzavírá Tomáš Hlavsa.

EVIDEN

Tomáš Hlavsa,
vedoucí oddělení Big Data & Security
a bezpečnostní ředitel společnosti Eviden

TŘI Z PĚTI českých zaměstnanců chtějí využívat umělou inteligenci v práci. Microsoft zjistil, jak se svět připravuje na příchod AI do práce

Umělá inteligence (AI) v posledních měsících dominuje v otázkách budoucnosti pracovního trhu. Pro společnost Microsoft je inovace v pracovním prostředí klíčové téma, proto se rozhodla v letošním Work Trend Indexu (WTI) zaměřit právě na AI v zaměstnání. Zjistila například, že více než polovina českých zaměstnanců si myslí, že v současnosti nedisponují vhodnými schopnostmi k výkonu své pracovní činnosti.

Průzkum Work Trend Index každoročně provádí Microsoft ve 31 vybraných zemích, ve kterých působí. Zároveň ale výsledky pro lepší porovnání rozčleňuje do jednotlivých států, a to včetně České republiky. Takto přináší unikátní porovnání, jak se přístup českých zaměstnanců a zaměstnavatelů liší v porovnání se světovým trendem.

Nástup umělé inteligence do pracovního prostředí okomentovala i Violeta Luca, generální ředitelka Microsoft Česká republika a Slovensko: „Umělá inteligence hraje výraznou roli v novém přístupu k práci. Stejně jako s nedávným nárůstem aplikací pro práci z domova se budou muset zaměstnanci naučit pracovat i s novými technologiemi využívajícími AI. Je to výzva i pro zaměstnavatele, kteří musí vyhodnotit, zda dává smysl nové AI doplňky implementovat do pracovních procesů. Správné zhodnocení situace je může v konkurenčním boji do budoucna zásadně zvýhodnit."

Až 60 % českých zaměstnanců v aktuálním Work Trend Indexu uvádí, že má problém s časem či energií na práci. Právě jim by mohla pomoci umělá inteligence, která dokáže usnadnit obzvláště repetitivní či administrativní činnosti. Přesto se část českých zaměstnanců k AI staví negativně. Až 34 % pracovníků se obává, že umělá inteligence nahradí jejich práci. Zajímavé je, že v porovnání se světovými daty jsou Češi zatím umírnění. Globálně se o svou práci v důsledku AI obává téměř polovina všech respondentů (49 %).

Na druhou stranu pracovníky, kteří se obávají o svou práci v důsledku AI, vysoce převyšuje procento zaměstnanců, kteří by umělou inteligenci v práci využívali a delegovali na ni co nejvíce úkolů. V Česku se počet zaměstnanců, kteří by AI užívali pro každodenní pracovní činnost, pohybuje kolem 59 %. Dvě třetiny Čechů by ji využívalo nejen pro administrativní úkoly, nýbrž i pro analytickou práci. Češi se v míře zapojení AI do pracovního života však ještě pohybují pod světovým průměrem, jelikož globálně by umělou inteligenci pro tento typ úkolů využívalo přes 75 % zaměstnanců.

Umělá inteligence by mohla pomoci především zaměstnancům s nedostatkem času a energie nebo s nesoustředěností. Tři pětiny českých zaměstnanců totiž mají pocit, že se během pracovního dne nedokáží soustředit. Globálně se toto číslo pohybuje kolem 68 %. Právě zaměstnanci s nedostatkem energie či s vysokou časovou vytížeností až 3,5× častěji celosvětově uvádějí, že mají problém s inovacemi a strategickým myšlením (v České republice je to jen 2,6×).

Stále se vyvíjející funkce a schopnosti umělé inteligence poukazují na nevyhnutelný trend, na který se musí připravit i zaměstnavatelé a vedoucí pracovníci. Právě ti totiž budou po zaměstnancích vyžadovat schopnost integrovat umělou inteligenci do každodenních pracovních činností. Až 78 % českých vedoucích pracovníků podle Work Trend Indexu společnosti Microsoft tvrdí, že v současnosti přijímaní zaměstnanci budou potřebovat nové dovednosti související s rostoucím vlivem AI. Pro srovnání, přibližně stejné procento zaměstnavatelů si totéž myslí i v Německu, Polsku či Velké Británii. Problematiku nedostatečných schopností pro práci s umělou inteligencí v zaměstnání dokládají sami pracovníci. Až 60 % zaměstnanců celosvětově uvádí, že jim tyto dovednosti chybí. V Česku se podle Work Trend Indexu jedná o 51 % zaměstnanců.

Microsoft se trendy a inovacemi v pracovním prostředí zabývá dlouhodobě. Pomocí celosvětového šetření Work Trend Index každoročně vyhodnocuje nejrůznější tendence pracovního trhu. V loňských letech se jednalo například o duševní pohodu v zaměstnání nebo hybridní práci. Zároveň vytváří nové aplikace a funkce, pomocí nichž se zaměstnanci mohou rychle se měnícímu pracovnímu prostředí přizpůsobit. Studie Work Trend Index se letos zúčastnilo 31 000 zaměstnanců, konkrétně 1 000 v každé z 31 zemí, kde společnost působí. Zaměstnanci pocházeli z Evropy, Asie a Severní a Latinské Ameriky.

Rozšíření portfolia společnosti Gordic o nové bezpečnostní produkty a služby

Na rok 2024 pro vás připravujeme podstatné rozšíření současného produktového portfolia bezpečnostních produktů. Informovali jsme o nich na konferenci Egovernment v Mikulově. Reagujeme tak na aktuální potřeby zákazníků i legislativní změny, které přináší směrnice NIS2. V nabídce přibudou postupně 3 nové produkty formou SaaS (Software as a Service) a posléze i na ně navázané MSSP (Managed Security Services Provider) služby. U všech z nich byla při jejich přípravě na prvním místě snaha o co nejsnazší nasazení, maximální využití již používaných bezpečnostních technologií a bezproblémová integrace s nimi a v neposlední řadě i snadná správa, atraktivní celkové náklady spojené s vlastnictvím a brzká návratnost investice.

Monitorování externí útočné plochy

Prvním z připravovaných produktů a návazných služeb je nástroj pro *Monitorování externí útočné plochy*. Díky němu získáte pohled kybernetického útočníka na svoje informační aktiva dostupná z internetu. Primárně se k jejich detekci využívá neinvazivní přístup (OSINT techniky). Díky tomu nehrozí, že byste si prováděnými testy ohrozili funkčnost svých publikovaných aktiv. Výsledkem práce je inventarizace vašich externích služeb, technologií, DNS, certifikátů, potenciálních zranitelností atd. Zvládá i monitoring obsahu tzv. Dark webu. Díky tomu máte přehled, zda se v temných zákoutích internetu neobchodují uniklé přihlašovací údaje uživatelů vaší společnosti nebo informace o vašich kompromitovaných aktivech. Třešničkou na dortu je pak funkce nákupu obchodovaných uniklých údajů z vybraných hackerských tržišť přímo z administrátorské konzole.

Dále lze jednoduše monitorovat podvodné domény nebo účty na sociálních sítích, které se snaží vystupovat jménem vaší společnosti. Zmiňovaná funkce nabízí kromě detekce podvodné domény nebo účtu i integrovaný tzv. „takedown". To znamená, že za definovaných okolností umíte jediným tlačítkem iniciovat odstranění podvodné domény či účtu. Pro pracovníky informační bezpečnosti ve vaší společnosti nabízí produkt i další benefity v podobě TI (Threat Intelligence) dat – informací o aktuální zranitelnosti produktů a jejich zneužívání, bezpečnostních incidentech dodavatelů, aktivitách APT skupin, analýzy malware, IoC (Indicators of Compromise), threat hunting rules atd.

Centrální správa bezpečnostních událostí

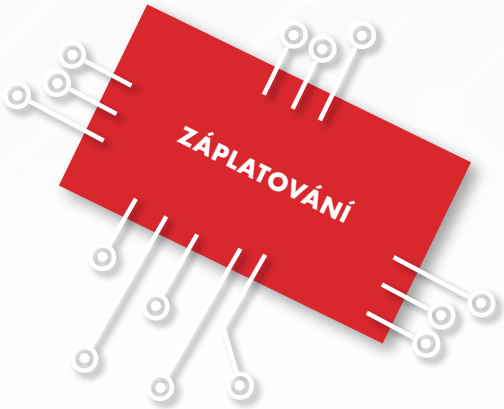
Druhý z produktů se bude specializovat na *Centrální správu bezpečnostních událostí a reakce na ně*. Každý manažer kybernetické bezpečnosti nebo IT manažer dříve či později narazí při snaze monitorovat dění ve svěřené IT infrastruktuře po stránce informační bezpečnosti na fakt, že jde o obrovské objemy a množství událostí, které je potřeba uložit, správně vyhodnotit a adekvátně na ně reagovat. Jak toho dosáhnout?

Naším řešením je využití otevřené konvergované bezpečnostní platformy integrující SIEM, E/XDR, SOAR. Není tak potřeba znehodnotit investice, které jsme do informačně bezpečnostních řešení již vložili v minulosti. Díky otevřenosti nabízené platformy naopak jejich výstupy jednoduše integrujete do jednoho funkčního celku.

O to, že budou data správně vyhodnocena a poskládána do smysluplných bezpečnostních událostí, se starají AI technologie v podobě neuronových sítí. I když je produkt nabízen primárně formou SaaS, zvládne monitoring jak vašeho cloud prostředí, tak i interní infrastruktury. Pro opravdu velké zákazníky s enormním množstvím zpracovávaných událostí i jejich objemu lze produkt nasadit a provozovat za definovaných podmínek i přímo na zákaznické infrastruktuře.

Záplatování aplikací a operačních systémů

Třetí a poslední připravovanou produktovou novinkou je *Záplatování aplikací a operačních systémů za běhu*. Co si pod tím představit? Hned několik zajímavých benefitů. Každý ze správců ICT zná situaci, kdy je objevena tzv. zranitelnost nultého dne, na kterou v tu chvíli neexistuje od dodavatele operačního systému nebo aplikace bezpečnostní záplata, a vy tak stojíte před otázkou, zda akceptovat riziko a čekat třeba dny či týdny na oficiální záplatu od výrobce, nebo zranitelnou službu odstavit.



Je tu však i chytrá třetí cesta v podobě nabízeného řešení, kdy se využije právě unikátní techniky záplatování za běhu. Záplaty na kritické zranitelnosti v operačním systému Windows jste díky tomu schopni, i bez příslušné záplaty od Microsoftu, mít nasazeny automaticky a bez vašeho zásahu již v řádu několika hodin. A vůbec nevadí, zda již máte implementován klasický záplatovací mechanismus, kdy typicky jednou měsíčně provádíte odstávku systémů spojenou s aplikací bezpečnostních záplat. Oba přístupy jsou vzájemně kompatibilní.

Záplatování za běhu vám rovněž může pomoci s naplněním SLA na služby, vámi poskytované, právě díky provozu bez odstávek. Dalším velkým benefitem je i skutečnost, že záplaty v rámci nabízeného řešení jsou poskytovány i na verze Windows, Microsoftem již nepodporované. Lze tak úspěšně vyřešit dilema, kdy máte v provozu kritickou business aplikaci běžící již na nepodporované verzi operačního systému. Stejně tak to může být i výrobní linka.

Nové legislativní povinnosti

Na konferenci v Mikulově jsme dále informovali o blížící se povinnosti z oblasti kybernetické bezpečnosti. Tou je zavedení evropské směrnice NIS2. I když se do českého zákona o kybernetické bezpečnosti promítne až v roce 2024, odborníci radí začít s přípravami už teď. Hlavním cílem je dosáhnout toho, aby organizace zaváděly preventivní kroky k posílení své kybernetické bezpečnosti a tím zvyšovaly bezpečnost důležité infrastruktury v celé EU.

Pro řadu organizací bývají nové povinnosti vyplývající z evropské legislativy náročné nejen finančně, ale také administrativně a procesně, a to i z důvodu složitého výkladu legislativních předpisů. Proto doporučujeme obrátit se na odborníky, kteří dokáží najít nejméně nákladné a efektivní řešení v souladu s evropskými požadavky.

Miroslav Dvořák,
ředitel odboru Správa informační bezpečnosti,
Gordic

GORDIC

CO ČEKÁ SPISOVÉ SLUŽBY

Posledním bodem programu mikulovské konference byla dopolední debata zaměřená na spisové služby, a především jejich atestace. Pozvali jsme si k ní* Petra Vokáče, *vrchního ředitele sekce legislativy a státní správy, MV ČR,* Karla Trpkoše, *vrchního ředitele sekce informačních technologií, MPSV ČR,* Petra Stieglera z *České agentury pro standardizaci,* Tomáše Bezoušku z *poradenské společnosti INADVISORS a Ladislava Mazače ze společnosti GORDIC. Chtěli jsme tak v rámci debaty pokrýt problematiku spisových služeb od těch, kteří je mají „v gesci", přes ty, kteří si je nasazují do úřadu, ty, kteří s takovými kroky radí, až k těm, kteří potřebné produkty dodávají. V rámci celého dopoledne zazněly jak prezentace, tak především odpovědi na otázky z publika, což celé generovalo řadu zajímavých informací.

Diskutující pánové se jednohlasně shodli na tom, že spisovou službu je možné nazvat jakousi páteří každého úřadu, neboť do něj vnáší informace, koordinuje jednotlivé kroky, spojuje oddělení úřadu navzájem i se světem venku a zároveň chrání přenášené informace a data. O její potřebě tedy není diskuze ani pochyb. Určité pochyby by se daly vyjádřit na adresu současné legislativy, která upravuje fungování a nakládání se spisovými službami. Samotný zákon o archivnictví sice není špatný, ale v době svého vzniku se musel přizpůsobovat různým podnětům, což ve svém výsledku vedlo k určitému zmatení pojmů.

Pojmy a dojmy

Jedním z takových důležitých pojmů je dokument a komponenta (to je termín, který se objevil letos v souvislosti s novelou vyhlášky o spisovnách, a je to jakýsi pokus o narovnání mezi terminologií národní legislativy o spisovnách, tedy zákona o archivnictví, a instrumenty evropskými, především nařízením eIDAS). Zatímco podle nařízení eIDAS je, při velkém zjednodušení, dokumentem jakýkoliv soubor (např. PDF), tak podle národního archivního zákona a jeho dlouhodobého vnímání je dokumentem celek, který přišel v nějaké zásilce – obálce. Typicky se jedná o dopis a jeho přílohy. Tento rozpor je řešen tak, že přílohy nazýváme v národním standardu částmi u analogových dokumentů nebo komponentami u dokumentů digitálních. Je otázkou, do jaké míry pojem komponenta zákonnou úpravu vylepšuje, ale v danou chvíli nebyla na úrovni prováděcích předpisů jiná možnost.

I další úpravy v našem zákoně jsou důsledkem určitého jeho slepování. Například rozlišení určených a ostatních veřejnoprávních původců. Podle zákona by se mělo jednat o instrument pro rozlišení toho, jakou míru povinností by měly mít jednotlivé druhy původců z hlediska vedení spisové služby. Ve výsledku je míra povinností pro všechny druhy původců, od malých obcí až po ministerstva, vlastně velice podobná. Navíc zákon o archivnictví obsahuje poměrně velký a neúnosný podíl metodiky a určité rigidity. Například ustanovení o uzavírání spisu je spíše než paragraf zákona metodický pokyn.

Další zajímavostí je samostatná evidence dokumentů. Archivní zákon tento pojem nezná, ten upravuje vyhláška. Paradoxně ale některé jiné zákony s tímto vyhláškovým pojmem pracují a vážou jej na agendové informační systémy – například systémy stavebního řízení. Je určitě legitimní, aby vedle spisové služby existovaly i jiné systémy, které spravují dokumenty. Otázkou ale je, zda by dnešní zákon o archivnictví neměl definovat jasnou sadu pravidel, která se vztahují na správu dokumentů v jakémkoliv systému. Tzn., zda by neměla existovat obecná úroveň pravidel, poté speciálnější pravidla pro spisovou službu a pravidla pro agendové informační systémy, včetně případné integrace. Bylo by tedy vhodné se do budoucna nad těmito skutečnostmi zamyslet poněkud koncepčněji, a to v případě, že by mělo dojít ke změně či nahrazování současného zákona novými předpisy. Další zajímavostí je samostatná evidence dokumentů. Archivní zákon tento pojem nezná, ten upravuje vyhláška. Paradoxně ale některé jiné zákony s tímto vyhláškovým pojmem pracují a vážou jej na agendové informační systémy – například systémy stavebního řízení. Je určitě legitimní aby vedle spisové služby existoval i jiné systémy, které spravují dokumenty otázkou ale je , zda by ten dnešní zákon o archívnictví neměl definovat jasnou sadu pravidel, které se vztahují na správu dokumentů v jakémkoliv systému. Tzn. jakási obecná úroveň pravidel a poté speciálnější pravidla pro spisovou službu a pravidla pro agendové informační systémy včetně případné integrace. Bylo tedy vhodné se do budoucna nad těmito skutečnostmi zamyslet poněkud koncepčněji a to v případě, že by mělo dojít ke změně či nahrazováním současného zákona novými předpisy.

Proč jsme to letos nespravili?

Již déle jak rok probíhá diskuze o změnách legislativy o spisovnách, vyhlášky a národního standardu. Je tedy otázkou, proč nedošlo k nápravě? Důvodem je především skutečnost, že na úrovni zákona by nebylo vhodné postupovat dalším „lepením". Pokud jsme se zabývali například vyhláškou o spisovnách a měnili ji, zaváděli pojem komponenta a zjednodušovali rozsah metadat, upravovali typový spis atp. nebo pokud jsme měnili národní standard, nezbývalo nám nic jiného než se pohybovat na bázi současného zákona, a především tyto předpisy dát do pořádku v souvislosti s blížícími se atestacemi. Jsme na začátku cesty, kdy jsme udělali nezbytné úpravy, které bylo potřeba udělat především kvůli atestacím. V mezích možného se povedlo upravit předpisy důstojně tak, aby byly jednotlivé požadavky atestovatelné

Co je atestace jednotlivých systémů spisových služeb?

Atestace spisových služeb byly do zákona zavedeny nedávno. Jejich základním účelem je posouzení souladu elektronického systému spisových služeb právě s požadavky zákona, vyhlášky a národního standardu. Důležité je, že předmětem atestace je systém spisové služby, tedy otázky, co umí konkrétní systém, nikoliv, co umí s instalovaným systémem dělat veřejnoprávní původce. I to je ale určitý dluh, neboť díky atestacím máme ošetřenu kvalitu informačních systémů, ale práci původců musíme ošetřit ještě dalšími opatřeními. Často se například hovoří o tom, že na úrovni veřejnoprávních původců velmi často chybí silnější postavení metodika spisové služby jako někoho, kdo by měl být blízko vedení veřejnoprávního původce, fungovat jako určitý interní auditor výkonu spisové služby a aby požíval náležité formální a procesní váhy v organizaci. To je určitě další výzvou pro případnou úpravu legislativy na úrovni zákona.

Atestace jsou tedy jednou z komponent pro zajišťování kvality výkonu veřejné správy v rámci používání spisové služby. Atestaci provádí atestační středisko, kterým byla určena Česká agentura pro standardizaci (ČAS).

Čím se atestace řídí:

Pro samotné atestace jsou důležité tyto normy:

- zákon č. 499/2004 Sb.;
- vyhláška č. 259/2012 Sb.;
- Národní standard pro eSSL (https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx);
- postup atestačního střediska a podmínky provádění atestace (https://www.mvcr.cz/soubor/10vmv-docx.aspx);
- provozní řád atestačního střediska (https://www.agentura-cas.cz/atestace/provozni-rad/).

Důležité je, že atestace se budou vztahovat pouze k informačním systémům používaným veřejnoprávními původci. Za začátek atestace je považována její objednávka, kterou zpravidla činí výrobce. Ve výsledku jde o soukromoprávní vztah, který má na svém výstupu zásadní veřejnoprávní důsledky. Proto postupy pro atestace musí upravovat určité opravné prostředky tak, aby měl výrobce možnost konzultovat s ČAS případné nedostatky, aby byla zajištěna transparentnost a férovost procesu.

Úplata byla stanovena MV ČR na částku 489 000,- Kč. Jde o částku, která vychází z nákladů atestačního střediska na atestace a předpokládaného ročního počtu objednávek.
Samotný atest má platnost stanovenou na období dvou let, což je rovněž bod častých diskuzí. Určitým kritickým ustanovením zákona v jeho současné podobě je pravidlo o zneplatnění vydaného atestu v situaci, kdy během jeho platnosti dojde ke změně legislativy. Atest by měl být v tomto případě zneplatněn do jednoho roku od této změny.
Protože se jedná o poněkud kontroverzní body, byla v letošním roce připravena dílčí technická novela archivního zákona, která by měla některé z parametrů atestací pozměnit.

Harmonogram

Proces atestací byl zahájen 1. 7. 2023, přičemž od 1. 7. 2024 bude platit zákaz nabízet, nebo dodávat veřejnoprávním původcům neatestovaný eSSL. A od 1. 1 2026 mohou veřejnoprávní původci využívat pouze atestované eSSL. Navrhovaná novela archivního zákona, která je stále ještě v připomínkovém řízení, by ještě mohla tyto termíny upravit. Konkrétně zákaz nabízet neatestované eSSL by mohl být odložen o půl roku na 1. 1. 2025 a povinnost původců by byla odložena na 1. 1. 2027. Dílčí změnou je ještě doplnění výjimky z režimu atestací pro eSSL, které zpracovávají utajované dokumenty. Důležitější změnou je ale odstranění onoho kritického pravidla zneplatnění atestu v případě, že dojde ke změně legislativy a požadavků na atestování. Toto zneplatnění by se nově nahradilo prostým prohlášením výrobce a informováním MV ČR a ČAS o tom, že i po změně legislativy zmiňovaný produkt nadále splňuje relevantní požadavky, jedná se tedy o důležité zjednodušení.
Technické novela by mohla být vládě a do dalšího legislativního procesu předložena na podzim tohoto roku. Vzhledem k tomu, že posouvá některé termíny, je důležité, aby byla účinná v první polovině příštího roku, což by se snad mělo stihnout.

Základní otázky k atestacím

- **Má mě atestace zajímat?**

Určitě ano, pokud jste dodavatelé nebo veřejnoprávní původci. To je samozřejmě velice široká skupina úřadů a zahrnuje i řadu subjektů, které mají vlastně jiný primární účel než výkon veřejné moci.

- **Co je atestace?**

Jedná se o posouzení eSSL s jinými předpisy či normami (zákon, vyhláška a národní standard). Požadavků, které se posuzují, je celkově přes 500. Všechny by měly být ověřeny a prozkoušeny, zda je spisová služba skutečně splňuje.
Atestací NENÍ! posouzení konkrétní implementace. Součástí ČASu není tým, který by chodil po úřadech a institucích a zjišťoval, zda konkrétní instalace je v souladu se zákonem, či jestli s ní veřejnoprávní původce zachází tak, jak by měl. ČAS zkoumá pouze prototyp konkrétní verze spisové služby. Atestace posuzuje soulad těchto prototypů pouze s předpisy, které se vztahují k výkonu spisové služby. Neřeší se tím otázka kybernetické bezpečnosti, ochrany osobních údajů atp.

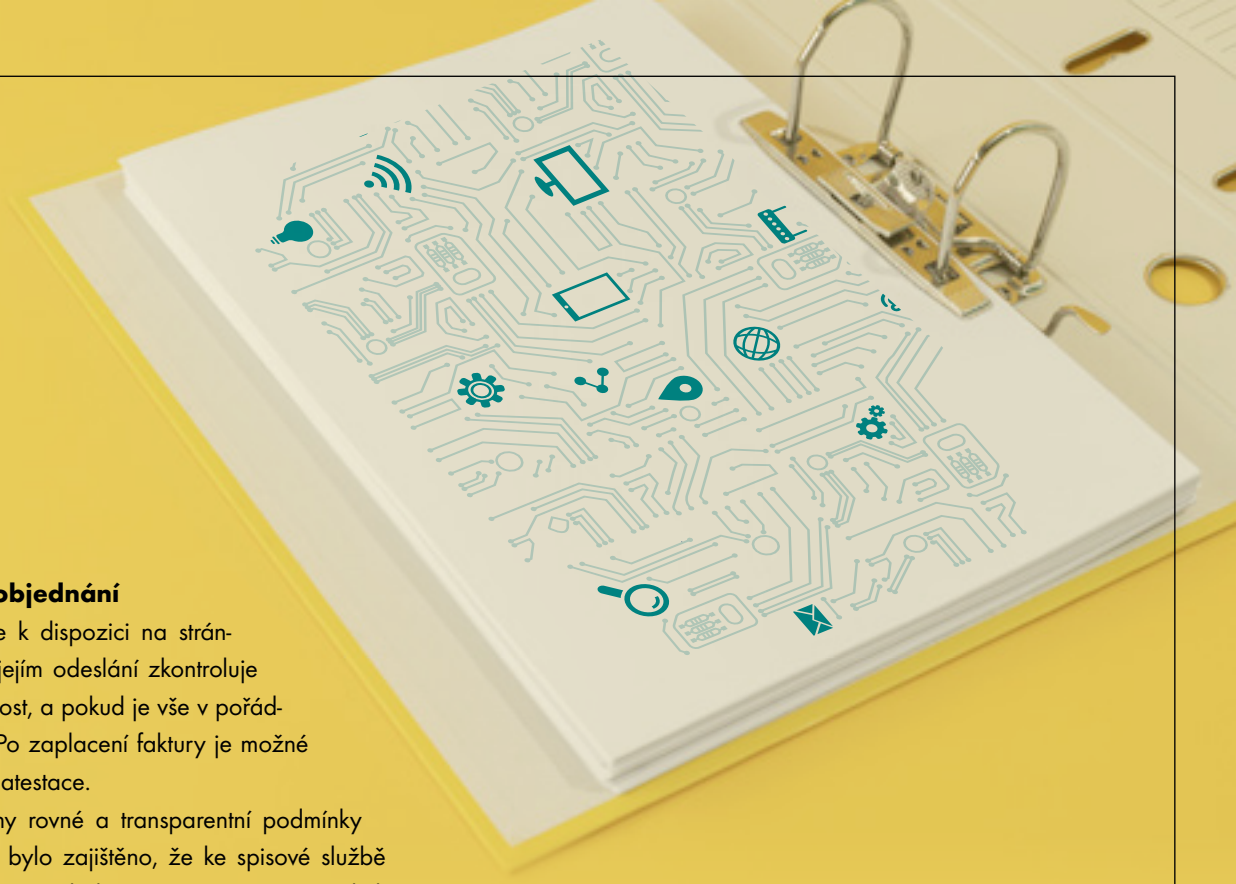
- **Kdo bude objednávat atestaci**

Nejčastěji výrobci a distributoři, protože atest potřebují, aby mohli výhledově spisovou službu nabízet a prodávat. V některých případech to ale také mohou být i veřejnoprávní původci, a to například ve chvíli, kdy mají nějaký systém od výrobce, který úřadu smluvně nezaručil zajištění atestací, nebo úřad vlastní tzv. o hybridní spisovou službu složenou z modulů různých výrobců.

Jak bude atestace probíhat

- **První fáze – příprava na straně objednatele**

Snahou ČAS a MV ČR není vytvořit nějaký bič k znepříjemnění, ale naopak nastavit vše tak, aby celý proces proběhl co nejhladčeji. I proto je atestační aparát veřejný a transparentní. Kdokoliv si může realizovat jakousi atestaci „nanečisto" sám na svém úřadu ještě před tím, než si objedná oficiální atestaci. Tento krok může úřadu poskytnout informaci o samotném stavu spisové služby a také dodat jistotu, že by eSSL měl atestací projít.
Před samotnou atestací je jednou z povinností vytvoření návodu. Atestace – tedy samotné testování - bude probíhat podle předem připravených atestačních scénářů, podle typických situací, které se odehrávají v rámci spisové služby a které by měly mít jasně definovaný predikovatelný výsledek. Ty jsou rovněž veřejné a k dispozici. Aby je testeři mohli odzkoušet, musí vědět, jak se konkrétní kroky realizují na konkrétní variantě eSSL. Tedy například kam kliknout pro založení spisu. Takový úkon bude u každého systému probíhat jinak, a proto je nutné zpracovat popis úkonů na konkrétní spisové službě. Velmi snadno je možné jej realizovat v rámci atestace nanečisto, která se bude zaznamenávat, a tento záznam může sloužit jako uvedený návod.



• **Druhá fáze – objednání**

Vzor objednávky je k dispozici na stránkách agentury. Po jejím odeslání zkontroluje agentura její náležitost, a pokud je vše v pořádku, vystaví fakturu. Po zaplacení faktury je možné přistoupit k procesu atestace.

Aby byly zachovány rovné a transparentní podmínky pro všechny a aby bylo zajištěno, že ke spisové službě nebude moci někdo v průběhu testu přistupovat a cokoli na ní upravovat, probíhají atestace v laboratorním prostředí agentury. To jakási virtualizovaná platforma, kam je testovaná spisová služba instalována.

• **Třetí fáze – instalace**

Většina atestací bude probíhat tak, že na základě konkrétních informací vytvoří ČAS prostředí, do kterého je možné spisovou službu instalovat. Vše bude protokolárně předáno a prostředí uzamknuto tak, aby nemohl nikdo další přistupovat, a je možné zahájit poslední fázi.

• **Čtvrtá fáze – atestace**

Atestace se realizuje podle předem daných, zveřejněných testovacích scénářů, které pokrývají všechny požadavky, jak bylo řečeno. Vyhodnocení je jednoduché splňuje/nesplňuje. Aby eSSL splnila atest, musí splňovat všechny uvedené požadavky. Proces tedy končí buď vydáním atestu, nebo existuje jakési odvolací řízení, které předchází vydání toho rozhodnutí, a je prostor k vyjádření či odvolání.

Provozní řád atestačního střediska

Informuje o tom, co stanovuje provozní řád atestačního střediska.

Část 1: Metodika přípravy atestačního prostředí

Stanovuje zásady, pravidla, požadavky a postupy pro provedení přípravy atestačního prostředí, tedy části procesu atestace od okamžiku jejího zahájení na základě akceptované objednávky do okamžiku předání do atestačního prostředí ze strany objednatele atestačnímu středisku k provedení testů.

Část 2: Testovací scénáře pro provedení atestace eSSL

Dokument „Testovací scénáře pro provedení atestace eSSL" je rozcestník a popis příloh: Příloha 1: „Výchozí nastavení eSSL před zahájením testování"; Příloha 2: „Testovací scénáře" (PDF + Excel).

Část 3: Bezpečnostní politika atestačního střediska

Stanovuje závazné zásady, pravidla, požadavky a postupy řízení informační bezpečnosti, jejichž cílem je chránit prostředky atestačního střediska, a to s ohledem na relevantní legislativní a organizační bezpečnostní požadavky.

Veškeré informace by měly být k nalezení na:

www.agentura-cas.cz/atestace; www.mvcr.cz/clanek/atestace-elektronickych-systemu-spisovych-sluzeb.aspx.
Kromě těchto témat odpovídali pánové na řadu dotazů z pléna.
Celý záznam diskuze naleznete na www.egovernment.cz sekce Mikulov23.

Fenomén spisovka

Začneme pojmem byrokracie. Pro vymezení pojmu byrokracie najdeme i tuto definici: „administrativní činnost, jejímiž znaky jsou systematičnost, specializované funkce, pevně stanovená pravidla pro činnost i výkon správy". Zákonem, který definuje tato pravidla, je v případě ČR správní řád. Ten nastavuje celý postup zpracování od podání přes řízení až po rozhodnutí. Další legislativní normy však stanoví podrobnosti, jak tyto činnosti vykonávat.

Základním nástrojem pro podporu těchto činností je *spisová služba*, jež v sobě odráží funkčnost byrokracie už od dob Rakouska-Uherska. Právě od této doby je v naší veřejné správě používán systém evidence celého životního cyklu dokumentů, záznamů, spisů apod., z něhož se vyvinula i dnešní spisová služba. V minulosti se používala v papírové podobě, dnes existuje řada počítačových aplikací na řešení této problematiky. Ty označujeme pojmem *elektronická spisová služba*, zkráceně eSSL. Již řadu let je v naší legislativě zakotveno, jakou funkčnost tyto aplikace mají mít a zároveň jaké povinnosti mají organizace pro realizaci agendy *spisové služby*. Díky tomu jsou v ČR různé eSSL poměrně rozšířené.

Elektronické systémy spisové služby patří do kategorie aplikací typu *Record Management*, jež poslední dobou zažívají velký rozmach i ve světě. Pořádek v dokumentaci, včetně důkazních prostředků a kvalitní archivace, se dostává do priorit IT v celé řadě odvětví. Velký důraz na tuto problematiku kladou vedle veřejné správy a finančních institucí (např. bank či pojišťoven) i průmyslové podniky.

Vraťme se ale zpět do oblasti veřejné správy. Dle priorit vlády musí být digitalizace nástrojem reformy státní správy, ne jejím cílem. Proto je nutné zjednodušit a zpřehlednit právní řád a zrychlit správní řízení. Otázkou je, zda eSSL je schopna tomu pomoci. Moje odpověď zní: pokusme se o to!

Klíč k digitalizaci veřejné správy

Nabídka aplikací eSSL je v ČR velmi široká, jak ale ukázala analýza Ministerstva vnitra, či kontrolní činnost příslušných archivů, s vlastním použitím těchto aplikací ve státních institucích to není slavné. Přitom platí, že eSSL patří pro organizace veřejné správy mezi páteřní nástroje, se kterými by měly komunikovat i další agendové informační systémy organizace.

Proto se nelze divit, že eSSL musí sehrát dominantní úlohu v rámci digitalizace služeb veřejné správy, která v současnosti patří k nejvyšším prioritám. Bylo řečeno, že pro dosažení tohoto cíle je nutno digitalizaci lépe řídit a koordinovat. Začaly se tedy objevovat úvahy o standardizaci aplikací, centralizaci apod. Tyto úvahy vznikly kvůli tomu, že na IT řešení je vynakládáno stále větší množství prostředků a je třeba zajistit, aby byly vynakládány efektivně a správně. V rámci těchto úvah se přetřásala řada dobrých i méně dobrých nápadů. Jedním z nich byla i atestace klíčových systémů, využívaných subjekty veřejné správy.

Cílem atestace obecně je prokázání způsobilosti, jakosti plnění či určité funkčnosti, jednoduše soulad s definovanými požadavky. Jakost nelze hodnotit intuitivně, ale je nutné hodnocení objektivizovat: stanovit měřitelné vlastnosti aplikace, pro které jsme schopni stanovit konkrétní požadavky.

Atestace ověřuje funkčnost

Právě atestace elektronických spisových služeb však nakonec sítem různých nápadů v rámci úvah o digitalizaci prošla. Proč právě ta?

Jedním z důvodů je, že na rozdíl od jiných případů, kde rozhodnutí o nasazení aplikace musí být vyváženým kompromisem mezi náklady na jeho pořízení, zavedení a provoz na jedné straně a užitkem, který přinese, na straně druhé, použití produktů eSSL bylo a bude u celé řady organizací veřejné správy povinností ze zákona. Druhým, a možná ještě pádnějším důvodem byla existence jasné legislativy, detailně popisující funkčnost eSSL, kterou bylo možno využít pro stanovení konkrétních požadavků.

Po několika letech vcelku náročných příprav je zde rok 2023 a atestace eSSL jsou realitou. Existuje legislativa, existuje i metodika, existuje také atestační středisko, kterým se stala Česká agentura pro standardizaci, a nad vším bdí Ministerstvo vnitra. Jsou stanoveny i důsledky nabízení, používání či nepoužívaní atestovaných a neatestovaných aplikací pro dodavatele i uživatele.

Na přípravě legislativy i metodiky se podíleli nejen odborníci z Ministerstva vnitra, Národního archivu a atestačního střediska, ale i dodavatelé eSSL v rámci pracovní skupiny ICT Unie. Odborná diskuse na toto téma byla dlouhá, někdy i bouřlivá, ale výsledkem je konsensuální řešení, které je použitelné pro praxi.

Jak již bylo řečeno, cílem bylo v rámci atestačního procesu nastavit takové podmínky, které jednak ověří všechny požadavky stanovené zákonem, vyhláškou a Národním standardem eSSL a zároveň zaručí objektivní a transparentní hodnocení všech atestovaných systémů. I proto byly všechny požadavky převedeny do konkrétních testovacích scénářů, které budou pro všechny atestované spisovky stejné, a navíc se s nimi každý může seznámit na webových stránkách atestačního střediska.

Příprava atestace ukázala, že se zdaleka nejedná o jednoduchou činnost. Nese s sebou velké nároky na odbornost a zkušenost, a stejně tak i její nemalé náklady na přípravu celého prostředí a přípravu HW a SW atestačního prostředí. Jedná se však o účelně vynaložené náklady, které zásadním způsobem zvýší právní jistotu veřejnoprávních původců, že jimi zvolený systém skutečně odpovídá všem zákonným požadavkům.

Miroslav Širl, Petr Stiegler

ČESKÁ AGENTURA PRO STANDARDIZACI

Jak vypočítat náklady na provoz informačního systému veřejné správy?

Pořízení a provoz informačního systému z pohledu finančního je v IT světě vyjadřován tzv. TCO (Total Cost of Ownership), tedy celkovými náklady na vlastnictví. Zahrnuje jak pořízení, tak i náklady spojené s provozem IT systému během specifického časového úseku. Problematiku celkových nákladů vlastnictví informačního systému veřejné správy (TCO ISVS) zevrubně popisuje Metodika výpočtu TCO ICT služeb veřejné správy vydaná odborem hlavního architekta. Aby bylo možné metodiku prakticky využít, vznikl pro tento účel eGC kalkulátor, který má za úkol zjednodušit celý proces výpočtu a provést porovnání různých variant provozu informačního systému veřejné správy.

Co je vlastně eGC kalkulátor?

eGC kalkulátor je nástroj pro vyčíslení a srovnání nákladů různých variant řešení. Ve své původní verzi vznikl hlavně pro porovnání řešení provozované ve vlastním datovém centru (tzv. on-premise) a v cloudu. S postupem doby byl rozšířen i o možnost kombinovaného, tedy hybridní řešení. V současné době je kalkulátor koncipován více obecně a lze jej využít zejména v těchto případech:

- při kalkulaci celkových nákladů informačního systému (IS) za určité období;
- jako přílohu k žádosti o realizaci ICT projektu informačního systému veřejné správy zasílanou na odbor hlavního architekta eGovermentu;
- při porovnávání nákladů různých variant řešení IS (on-premise, cloud, hybridní řešení);
- při modelování ekonomické výhodnosti různých cloud scénářů řešení IS;
- při porovnávání nákladů realizace a provozu IS při různých bezpečnostních úrovních daného IS (tj. např. lze zjistit, o kolik se zvednou náklady IS, jestliže bude přeřazen z bezpečnostní úrovně „vysoká“ do bezpečnostní úrovně „kritická“);
- při detailní analýze vlivu jednotlivých nákladových položek na náklady IS;
- při porovnání různých nabídek na realizaci a provoz IS v rámci výběrového řízení.

Pro koho je eGC kalkulátor určen?

Kalkulátor je určen pro každého uživatele zajímající se o ekonomickou stránku provozu IT systémů. Vstupy do kalkulátoru může zadávat jak ekonom, tak i IT specialista, nicméně znalosti nezbytné pro správné zadávání potřebných údajů vyžadují znalosti jak z oblasti finanční, tak i z oblasti informačních technologií. Výstupní údaje jsou k dispozici jak v granulární formě s rozpadem nákladů dle metodiky pro finanční analytiky, tak i v přehledné a jednoduché formě srozumitelné finančním ředitelům a vedoucím pracovníkům.

Celková koncepce eGC kalkulátoru

Jak již bylo řečeno, eGC kalkulátor je jednotný nástroj pro kalkulace celkových nákladů vlastnictví (TCO) informačního systému, úspor a/nebo ztrát při provozu služby v modelu on-premise, cloudu nebo v hybridním řešení.

Při jeho tvorbě byly vzaty do úvahy následující předpoklady:

- kalkulace předpokládá 1 až 5leté období TCO;
- porovnání je mezi modelem „on-premise" a „cloudem". On-premise lze chápat tak, že služba je „seskládána" z komponent pořízených nákupem a zprovozněna formou systémové integrace. Cloud může poskytovat analogicky stejnou službu jako hotovou a připravenou k použití nebo je ke cloudu možné kalkulovat některé další položky navíc, a to takové, které cloudový poskytovatel nedodává (např. projektový management apod.);
- cloudová služba se rozumí ve variantě IaaS, PaaS nebo SaaS, tzn. všechny modely, které přicházejí do úvahy;
- kalkulátor může být použit i pro výpočet TCO hybridního řešení kombinujícího službu v cloudu s on-premise řešením.

eGC kalkulátor byl vytvořen v MS Excelu, pracovat s ním můžete jak v on-line, tak off-lie režimu. Tvoří jej 6 listů a koncepčně byl navržen tak, aby práce s ním byla maximálně intuitivní.

Klíčové vlastnosti eGC kalkulátoru

- eGC kalkulátor je nástroj pro vyčíslení a srovnání nákladů různých variant řešení; neprovádí kontrolu, zda je konkrétní položka (například server) vstupující do výpočtu pořízena levně nebo draze.
- eGC kalkulátor má za úkol mapovat a zviditelnit strukturu nákladů na provoz IS, která může být skryta pod jedním údajem; **poukazuje na položky, které marginálně ovlivňují TCO**.
- eGC kalkulátor nekontroluje na webu ani neodesílá zadaná data mimo kalkulátor; vše zůstává na jediném místě jako součást kalkulátoru.
- **Čím přesnější údaje do kalkulátoru vložím, tím přesnější je porovnání jednotlivých variant** s cílem přiblížit toto porovnání skutečnému stavu. Neúmyslné, případně záměrné uvádění nepřesných nákladových položek zkreslí finální porovnání.
- **eGC kalkulátor cíleně neprovádí žádné optimalizace vstupních hodnot;** může sloužit jako podkladový dokument pro optimalizaci a rozvoj informačního systému s ohledem na jeho náklady.

V řadě případů nejsou vstupní hodnoty při kalkulaci TCO známé. I na tento fakt kalkulátor pamatuje, a proto je možné použít hodnoty přibližné; do kalkulátoru lze uvést, že jde o odhad.

Co říci závěrem?

eGC kalkulátor určitě vyzkoušejte! Je k dispozici zdarma a jediné, co potřebujete, je tabulkový kalkulátor MS Excel a základní znalosti práce s ním.

Petr Leština,
manažer IBM pro Cloud

IBM

Odkazy:

- **eGC kalkulátor:** https://www.dia.gov.cz/wp-content/uploads/2023/08/eGC-TCO-eGC-Cloud-kalkulator_9-8-2023_final-1.xlsx
- **Uživatelská příručka:** https://www.dia.gov.cz/wp-content/uploads/2023/08/21-08-2023_Uzivatelska-prirucka_Metodika-TCO-ICT-v3.10-Priloha-c.1.pdf
- **Metodika výpočtu TCO ICT služeb:** https://archi.gov.cz/_media/dokumenty:metodika_tco_ict_sluzeb_vs.pdf

Distributed Cloud Services

Secure and optimize
apps and APIs anywhere.