Egovernment
elektronizace veřejné správy

Co se stalo v digitalizaci?

CO SE (TO) STALO?

Tak jako každý rok i letos jsme se sešli, tentokráte po šestnácté, na zámku Mikulov, abychom společně v příjemné atmosféře diskutovali nad tím, co se stalo v e-governmentu za uplynulý rok. Tento záměr podtrhoval i název úvodní prezentace vicepremiéra pro digitalizaci Ivana Bartoše, která měla být právě oním výčtem realizovaného za uplynulé období. Patrně ani on v tom okamžiku ještě netušil, že důležité, a hlavně dramatické, události pro elektronizaci veřejné správy se teprve blíží. Pár dní po naší konferenci proběhly volby do krajů s nevalným výsledkem pro Piráty, a následně si premiér přečetl expertní posouzení dosavadní digitalizace stavebního řízení a seznal, že Ivan Bartoš není schopen dále manažersky vést uvedený projekt a z pozice vicepremiéra pro digitalizaci jej odvolal. Výsledkem je skutečnost, že dalším vedením digitalizace stavebního řízení byl pověřen ministr dopravy Martin Kupka. A zatím to vypadá, že zažijeme jakési přechodné období, kdy bude možné používat nové i staré systémy, nicméně žádosti by nadále měly být podávány jen v elektronické podobě. Nyní se řeší především otázka, zda pokračovat v dosavadním směru, nebo se vrátit na začátek, včetně nového výběrového řízení.

Je naprosto logické, že hlavní pozornost na sebe nyní strhává právě digitalizace stavebního řízení. Konec konců se jednalo o jeden ze základních kamenů, který měl ukázat, že právě digitalizace agend je tou správnou cestou ke spokojenosti všech. Ale není to jen DSŘ, ale celková digitalizace veřejné správy, která je jakýmsi pilířem modernizace státu. A tak otázkou zůstává, co ta ostatní digitalizace? Kdo ji bude mít na starosti? Kdysi měla pozici samostatného ministerstva, tedy byla jedním z členů vlády, i když nikoli nejsilnějším. Později byla převedena pod MV ČR, které má sice v rámci vlády silnou pozici, ale zde byla jedním z mnoha témat, kterým se ministerstvo muselo věnovat. Následně měla vláda svého zmocněnce pro digitalizaci a v době nedávné byla digitalizace „vytažena" pod vicepremiéra, tedy, alespoň vizuálně, významem nad všechna ministerstva a zároveň byla vytvořena digitální agentura, která jednotlivé projekty realizuje. Byl tak do jisté míry podtržen význam digitalizace, která by se měla týkat všech resortů sjednoceně.

Víme tedy, co stalo za uplynulý rok, a především pak za několik málo uplynulých dní. Otázkou však je, co se stane dál? Kdo bude zodpovědný za celkovou digitalizaci, a tedy realizaci elektronizace veřejné správy? Padne ta tíha na Digitální agenturu, nebo ji naopak převezme na svá bedra premiér? Doufejme, že se brzy vyjasní.

Michal Jirkovský,
šéfredaktor

Obsah

Redakce	ÚVODNÍ SLOVO	3
	OBSAH, TIRÁŽ	4

CO SE STALO V DIGITÁLNÍCH SLUŽBÁCH ZA UPLYNULÝ ROK	6–7
DIA PŘEDSTAVILA KLÍČOVÉ PRIORITY NA DALŠÍ OBDOBÍ	8–10
ZMĚNA NEJEN VE VEDENÍ DIGITALIZACE STAVEBNÍHO ŘÍZENÍ	12–13
LITERÁRNÍ KOUTEK V MIKULOVĚ	14–15
NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI	16–17
KVALIFIKOVANÍ A NEKVALIFIKOVANÍ POSKYTOVATELÉ SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU	18–19
NÁVRAT DO KANCELÁŘÍ, NEBO HOME OFFICE?	20–23
GORDIC PŘEDSTAVIL AKTUÁLNÍ TRENDY V IS VEŘEJNÉ SPRÁVY	24–25
WATSONX.AI: GENERATIVNÍ UMĚLÁ INTELIGENCE	26–27
STRATEGIE PRO SPRÁVU DAT: PRŮVODCE NA CESTĚ K DOBRÉ PRÁCI S DATY	28–30

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

Šéfredaktor: Ing. Michal Jirkovský
Asistentka: Zdeňka Borecká

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

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.

Váš švýcarský nůž v oblasti doručování aplikací, aplikační bezpečnosti a zabezpečeného přístupu k aplikacím

Load Balancing


L3 a L7 DDOS ochrana


Bezpečný přístup k aplikacím


Global Load Balancing

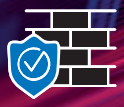

Firewall


Anti-fraud & anti-bot ochrana


Měření výkonnosti aplikací


SSL dekrypce a orchestrace


Web/Aplikační server


Web/Aplikační Firewall


Enkrypce uživatelských jmen


API Gateway


K8s Ingress controller


Automatizace CI/CD


API Management

Podpora všech veřejných Cloudů


Podpora hybridního cloudu


Managed Kubernetes


BIG-IP


Distributed Cloud Services


NGINX
Part of F5

CO SE STALO V DIGITÁLNÍCH SLUŽBÁCH ZA UPLYNULÝ ROK

Úvodní prezentaci letošního ročníku konference e-government 20:10 na zámku Mikulov měl na svých bedrech tehdy ještě vicepremiér pro digitalizaci a ministr pro místní rozvoj Ivan Bartoš. Co se stalo za uplynulý rok v digitalizaci to nebyla tedy ani tak otázka, ale skutečně spíše výčet událostí a zároveň název prezentace. Protože účastníci konference dali svým hlasováním najevo, v této době zcela pochopitelně, že mají největší zájem o informace týkající se probíhající digitalizace stavebního řízení, vicepremiér je ujistil, že se mu bude věnovat, ale svojí prezentací by rád shrnul, co vše se od loňské mikulovské konference změnilo. Stalo se tak necelé tři týdny před zásadní změnou, tedy jeho odvoláním z funkce a převedení agendy digitalizace pod ministra dopravy!

DIA FUNGUJE

Ivan Bartoš nejprve hovořil o Digitální informační agentuře, která existuje již rok a půl a díky které se „rozjely" některé zásadní projekty, které, jak uvedl, do té doby dlouho stagnovaly. Za zásadní považuje skutečnost, že se nyní daří překlenovat v ČR historicky zakořeněný resortismus a propojovat důležité agendy napříč rezorty. V tomto smyslu ukázkovým, podle jeho slov, může být projekt REZA.

eDOKLADY

Významným projektem, který byl v uplynulém období spuštěn, jsou eDOKLADY. Kromě samotného zaměření projektu vyzdvihl Ivan Bartoš především formu, jakou byl napsán příslušný zákon, který umožňuje postupný náběh a dobrovolné zapojování jednotlivých institucí a subjektů. eDoklady byly spuštěny v lednu 2024 a v době konání mikulovské konference (září 2024) mají 500 tisíc uživatelů. Začátek prázdnin, konkrétně 1. 7. 2024, byl dalším důležitým datem pro eDoklady, neboť došlo k rozšíření počtu ověřovatelů o úřady práce, finanční úřady, kraje a obce s rozšířenou působností, soudy a policii. Kromě toho k projektu přistoupila i řada soukromých subjektů z řad mobilních operátorů či bank. Vzhledem k často pokládaným dotazům, zda aplikace eDoklady bude obsahovat vedle OP i ŘP, uvedl Ivan Bartoš, že to není plánováno. A to i s ohledem na skutečnost, že na území ČR není povinnost mít řidičský průkaz při sobě, neboť policie může realizovat ztotožnění jiným dokladem a potřebné údaje dohledat. Naopak se ale uvažuje o zařazení potvrzení o studiu, stejně jako průkazu zdravotního postižení.

Ivan Bartoš vyzdvihl, že právě díky aplikaci eDoklady patří ČR do jisté míry k průkopníkům přípravy evropské peněženky – eWallet. Uvedl, že právě v této oblasti Česká republika podepsala memorandum o spolupráci mezi DIA a Dánskou agenturou pro digitální správu.

PORTÁL OBČANA (PO)

Ivan Bartoš upozornil na vylepšenou verzi a na spuštění mobilní aplikace PO. Obojí se odrazilo na nárůstu počtu služeb, a především počtu uživatelů. Zatímco v roce 2019 obsahoval Portál občana zhruba 29 základních služeb a využilo jej 45 000 uživatelů, v roce 2024 obsahuje již 100 služeb přímo a 600 zprostředkovaně, přičemž počet uživatelů dosahuje 1 400 000. Důležité je si uvědomit, že toto je číslo, které se týká skutečně pouze těch, kteří využí-

vají Portál občana. Vedle toho je zde řada dalších uživatelů digitálních služeb veřejné správy, kteří k jednotlivým službám (např. Moje daně) přistupují přímo, a tedy bez tohoto portálu. Ze statistik vyplývá, že nyní 76 % občanů alespoň jednou v roce využije nějakou digitální službu státu.

REGISTR ZASTUPOVÁNÍ

V souvislosti s realizací tohoto projektu Ivan Bartoš poděkoval spolupracujícím rezortům. Prvním, kdo bude čerpat výhody do tohoto zapojení, je ministerstvo dopravy. Dále se aktuálně řeší zapojení MPSV. Jedná se o projekt, který je důležitý například i pro zmiňované stavební řízení. Portál stavebníka bude totiž nyní moci pracovat s jednotlivými rolemi, které jsme doposud museli dokládat pouze předložením papírové plné moci. Stejně tak, díky projektu REZA, začnou fungovat tzv. implicitní mandáty, které jsou dány vazbou jednotlivých registrů – například, když rodič zastupuje dítě atp.

GOV.CZ

Z pohledu kyberbezpečnosti je velice důležitým projektem přechod na jednotnou vládní doménu GOV.CZ. Občané tak budou mít skutečně jistotu, že komunikují se státní institucí, což je zcela zásadní. Doposud na tuto doménu přešlo 100 úřadů a celková migrace by měla být dokončena do roku 2025.

eTURISTA

Jde o projekt, který byl rovněž obsažen v Národním plánu obnovy. Jedná se o registr obyvatel, díky kterému je možné naplnit jednotlivé funkce a povinnosti, které obyvatelé vůči státu a obcím mají. Odstraní se tak zbytečné papírování, například u agend místních poplatků či informací pro MV o pobytu cizinců, nebo usnadní získávání dat důležitých pro statistický úřad. Zároveň tak bude možné evidovat, a tedy regulovat, aktivity v oblasti sdíleného bydlení/ ubytování (Airbnb).

DIGITALIZACE STAVEBNÍHO ŘÍZENÍ

Jedná se o projekt, o kterém se diskutovalo již velice dlouho před samotným zlomovým datem, kterým bylo 1. 7. 2024. Podle slov Ivana Bartoše tato myšlenka ležela před rekodifikací stavebního práva na Ministerstvu pro místní rozvoj už přibližně od roku 2014. Připomenul, že Digitalizace stavebního řízení je podmínkou pro plnění Plánu obnovy a zároveň shrnul poněkud komplikovanou cestu projednávání zákona v Poslanecké sněmovně, jakož i jeho schválení „po termínu", změnu architektury, soutěžení, a nakonec dohadování s antimonopolním úřadem. I to byly důvody, proč systém v současné době vykazuje určité potíže. Jak Ivan Bartoš uvedl, některé z těchto potíží jsme možná mohli očekávat, u některých to mohlo být překvapení. Ale současný stav je takový, že všechny dotčené úřady, kterých je cca 1600, byly připojeny a mohou přijímat dokumenty a pracovat s nimi.

DŮLEŽITÉ SOUVISLOSTI

Vláda věnuje pozornost posilování infrastruktury státu. V jistém smyslu se srdcem české digitalizace stávají nejen základní registry, ale i komponenty ověřující identitu. To je důležité pro rozšiřování služeb státu, a i proto byla navýšena kapacita NIA (Národní identifikační autorita).
Stejně jako jiné země i ČR má problém se získáváním kvalitních IT odborníků do veřejné správy. I proto jsou důležité různé osvětové akce, které do jisté míry popularizují eGovernment.
A jako velice důležité téma Ivan Bartoš na závěr vyzdvihl Zákon o právu na digitální službu, který v plnou platnost „naskočí" v roce 2025. Vzhledem k tomu, že se jedná o zastřešující dokument celé digitalizace, dohlíží DIA na celý proces implementace, nicméně stále platí, že jsou některé služby, které digitalizovat nejdou a nikdy digitalizovány nebudou.

NA KONFERENCI EGOVERNMENTU V MIKULOVĚ PŘEDSTAVILA DIA SVÉ KLÍČOVÉ PRIORIITY NA DALŠÍ OBDOBÍ

Na tradiční konferenci eGovernmentu v Mikulově, která se konala od 2. do 4. září 2024, reflektovala Digitální a informační agentura (DIA) svou činnost za uplynulý rok a představila své klíčové priority na další období. Mezi ně patří věcné převzetí správy Registru obyvatel a Registru osob od MV a ČSÚ k 1. 11. 2024, zahájení prací na architektuře základních registrů nové generace a pomoc úřadům a institucím v postupném připojování do Registru zastupování. Dále pak pomoc úřadům a institucím v přípravě na Zákon o právu na digitální služby, který vstupuje v účinnost 1. 2. 2025, stanovení priority dalšího rozvoje NIA a příprava na implementaci evropské digitální peněženky v České republice.

DIA na konferenci eGovernmentu, která se konala první zářijový týden na zámku v Mikulově, seznámila účastníky s klíčovými projekty digitalizace státní správy, na kterých se z pozice nadresortního koordinátora podílí.

Ředitel agentury **Martin Mesršmíd** zde představil projekty, na kterých v uplynulém roce DIA intenzivně pracovala, na kterých aktuálně pracuje a na které se připravuje. Prioritou agentury je podpora nadresortních projektů, jako je například příprava úřadů a institucí na Zákon o právu na digitální služby. Tento zákon má za cíl zásadně změnit způsob poskytování veřejných služeb a umožnit občanům komunikovat s úřady čistě digitální formou. Předpokládá digitalizaci mnoha služeb státního sektoru, která vyžaduje velké finanční i lidské zdroje, a také čas. V současnosti probíhá implementační etapa, ve které se řeší nové rozhraní pro vyhledávání služeb či propojení s životními situacemi.

Dalším z aktuálních projektů DIA je spuštění Registru zastupování (REZA), který umožní úřadům efektivně spravovat oprávnění k jednání za jiné osoby. *„REZA je přelomový nástroj, který umožní činit digitální úkony v zastoupení. Aktuálně probíhá plnění připraveného registru daty, aby jej občané mohli podle postupného zapojení jednotlivých resortů co nejdříve využívat,“* dodal ředitel DIA Martin Mesršmíd, který zároveň představil harmonogram činností v projektu. Zvláštní apel směřoval na ministerstva a další státní instituce, aby se aktivně do REZA zapojily, podobně jako to již provádí Ministerstvo dopravy. REZA

„REZA je přelomový nástroj, který umožní činit digitální úkony v zastoupení.“

bude možné v budoucnu využít i pro zplnomocnění při podání daňového přiznání či žádosti o cestovní pasy dětí. Spolupráce mezi jednotlivými institucemi je klíčová i pro úspěšné spuštění třetí fáze eDokladů, plánované od ledna

2025. Aplikaci eDoklady, která umožňuje občanům prokazovat na místě svoji totožnost digitálně a bezpečně, si stáhlo již přes 500 000 uživatelů a v současnosti je akceptována na všech ústředních správních úřadech, krajích a obcích s rozšířenou působností či na různých úřadech jako jsou např. živnostenské úřady, katastrální, finanční, úřady práce aj. Od dubna 2024 začala eDoklady akceptovat Police ČR při práci v terénu, od července i na služebnách. Od třetí fáze bude možné použít eDoklady i ve školách, bankách, při volbách či na poště.

DIA dále zahájí práce na architektuře nové generace základních registrů, která zajistí jejich dlouhodobou udržitelnost. Je třeba si znovu definovat význam základních registrů a jejich způsob využití a vybudovat novou architekturu, která bude sloužit dalších 15 let, neboť stávající registry fungují již od roku 2012. Jedná se o velký projekt, kdy bude třeba široké otevřené spolupráce mnoha subjektů (státních i komerčních). V současnosti se již zahajují práce na referenční architektuře.

Významným bodem je také další rozvoj Národní identitní autority (NIA), která hraje klíčovou roli v bezpečné vzdálené autentizaci uživatelů v rámci digitálních služeb státu. Navýšení její kapacity bylo nutné již při spuštění eDokladů, kdy se rázem začalo autentizovat velké množství uživatelů. Aktuálně probíhá studie možností dalšího rozvoje NIA, kdy se zvažují různé alternativy provedení a probíhá příprava národního bodu pro hybridní provoz.

V souvislosti s implementací evropské digitální peněženky (EUDIW) v České republice, která musí být spuštěna do podzimu roku 2026, upozornil Martin Mesršmíd, že na provedení nutných legislativních změn a vybudování potřebné státní infrastruktury zbývají jen dva roky a agentura má před sebou ještě mnoho práce. *„Implementace EUDIW je jedním z našich nejdůležitějších projektů. Evropská digitální peněženka umožní občanům uchovávat a sdílet své digitální identity a klíčové osobní údaje v bezpečné a uživatelsky přívětivé formě ve všech zemích EU,“* uvedl dále. V projektu proběhly již potřebné analýzy, ustanovily se pracovní skupiny a nyní se kromě legislativních změn pracuje i na vybudování backendové státní části EUDIW, připravuje se soutěž na provozovatele aplikační části EUDIW či byl spuštěn nový web EUDIW (eudiw.dia.gov.cz), kde jsou pro veřejnost dostupné informace včetně aktualit týkajících se EUDIW.

„Evropská digitální peněženka umožní občanům uchovávat a sdílet své digitální identity a klíčové osobní údaje v bezpečné a uživatelsky přívětivé formě ve všech zemích EU.“

DIA od svého vzniku stihla dosáhnout řady úspěchů. Kromě spuštění a rozvoje eDokladů mezi ně patří také rozšíření funkcionalit Portálu občana, který se stává stále důležitějším nástrojem pro komunikaci občanů s veřejnou správou. Na jaře 2024 byla spuštěna i mobilní aplikace Portálu občana pro jeho pohodlnější používání na mobilních telefonech. O zvyšujícím se využívání Portálu občana svědčí i statistika, kdy DIA oproti prosinci 2023 zaznamenala v červenci 2024 36% nárůst registrovaných uživatelů a 56% nárůst přihlášení.

Zásadním a klíčovým projektem bylo pro DIA zřízení kompetenčních center, která poskytují odbornou podporu úřa-

„Děkuji všem, kteří přispívají k digitalizaci veřejné správy. Naše společné úsilí přináší dobré výsledky, ale pořád je co zlepšovat."

dům při realizaci digitálních projektů. Cílem je pomáhat s projekty od začátku až po akceptaci a přenášet zkušenosti z jednoho úřadu na druhý. Aktuálně tým kompetenčních center tvoří cca 50 odborníků, v budoucnu se bude skládat až z 80 profesionálů. Ti již dnes pomáhají např. na novém portálu Ministerstva vnitra, Policie ČR a Hasičského záchranného sboru ČR, zpracovávají analýzu uživatelských potřeb pro Ministerstvo dopravy či provádějí konzultace s Ministerstvem školství, mládeže a tělovýchovy v souvislosti s přípravou při budování nového informačního systému vzdělávání.

DIA se také intenzivně připravuje na převod Registru osob a Registru obyvatel z gesce Českého statistického úřadu a Ministerstva vnitra. Převod, který se uskuteční 1. 11. 2024, zajistí efektivní plánování a financování rozvoje a obnovy těchto klíčových registrů „pod jednou střechou".

DIA velmi oceňuje práci organizátorů konference eGovernmentu, která každoročně shromažďuje všechny, kteří se na digitalizaci státu aktivně podílejí. *„Děkuji všem, kteří přispívají k digitalizaci veřejné správy. Naše společné úsilí přináší dobré výsledky, ale pořád je co zlepšovat. Je potřeba vytvořit prostředí, které bude pro digitalizaci příznivější, ať už se jedná o schopnost státu lépe sdílet získané zkušenosti napříč resorty, získat potřebné odborníky, snadněji vysoutěžit jednotlivé zakázky nebo lépe koordinovat celé projekty,"* uzavřel Martin Mesršmíd.

isss 2025

12.–13.5.25
HradecKrálové
Kongresové centrum **Aldis**

27. ročník mezinárodní konference zaměřené
na **digitalizaci veřejné správy** a **rozvoj e-governmentu**







Více informací a registrace na
www.isss.cz

pořadatel
TRIÁDA

spolupořadatel
Kraj Vysočina

spolupracují
KRÁLOVÉHRADECKÝ KRAJ
HRADEC KRÁLOVÉ
CHRÁMOVÝ REGINA

isss.cz #issscz @issscz triadasro isss-konference

ZMĚNA NEJEN VE VEDENÍ DIGITALIZACE STAVEBNÍHO ŘÍZENÍ

Na konferenci v Mikulově vystupoval rovněž ministr dopravy Martin Kupka s přehledem aktuální digitalizace v rámci jeho resortu. Toto vystoupení, spolu se všemi ostatními, máte k dispozici na webových stránkách Magazínu Egovernment, v sekci Mikulov 2024. Pro digitalizaci je ovšem podstatnější jeho role, kterou zaujal ve dnech následujících po konferenci.

Po výsledcích krajských voleb, ale především po prostudování expertní studie digitalizace stavebního řízení, vystoupil premiér vlády ČR Petr Fiala s tímto prohlášením: *„Po zralé úvaze jsem se rozhodl, že podle článku 68, odstavce 5 a článku 74 Ústavy České republiky navrhnu prezidentu republiky odvolání Ivana Bartoše z pozice vicepremiéra pro digitalizaci a ministra pro místní rozvoj ke 30. září tohoto roku."*

Důvodem pro tento krok bylo projednání analýzy digitálního stavebního řízení vládou, a především pak osobní rozhovor mezi premiérem a vicepremiérem. Petr Fiala na základě těchto důvodů nabyl jistoty, že Ivan Bartoš není schopen digitalizaci stavebního řízení manažersky dotáhnout do úspěšného konce a, jak řekl, *„Myslím, že si ani nepřipouští, v jak reálném stavu proces digitalizace nyní je."* Dalším řízením projektu DSŘ byl pověřen ministr dopravy Martin Kupka, který následně na tiskové konferenci uvedl: „Vyhovíme opakovaným požadavkům stavebních úřadů a stavebníků a navrhneme legislativní řešení, které umožní používat původní nástroje stavebního řízení. Dále je naším úkolem stabilizovat systém, nesmí se objevit už žádné překotné aktualizace, které vedou ke zpomalení nebo zhoršení stávajících funkcionalit. Zásadním způsobem se také posílí testování samotnými uživateli, aby všechny systémy fungovaly tak, jak mají."

VARIANTA B – NOVÁ SOUTĚŽ

Po krátkém čase, který měli na analyzování situace ministr dopravy Martin Kupka a ministr pro místní rozvoj Petr Kulhánek, 16.10. 2024 představili vládě návrh řešení problémů spojených s digitalizací stavebního řízení (DSŘ). Tento krok je reakcí na aktuální stav, kdy systémy nenaplňují očekávání uživatelů a zákonné požadavky.

„Digitalizace stavebního řízení je klíčová pro zjednodušení a urychlení procesů územního plánování a povolování staveb. Naším cílem je zajistit, aby systémy byly uživatelsky přívětivé a plně funkční. Navrhli jsme proto částečný legislativní a technologický bypass, který umožní, aby stavební úřady po přechodnou dobu nahradily chybějící funkcionality ISSŘ doposud užívanými systémy," říká ministr dopravy **Martin Kupka**, který měl koordinační úlohu přípravy řešení digitalizace stavebního řízení a jehož role tímto končí.

„Náš návrh obsahuje dvě varianty dalšího postupu. Ve variantě A jsme posuzovali možnost pokračování v rozvoji systému. V rámci IT hodnocení i z hlediska hodnocení veřejného zadávání jsme tuto variantu vyhodnotili jako méně vhodnou než variantu B, kterou je nová cesta k cílovému řešení. Z pohledu veřejného zadávání se jedná o poptávání kapacit prostřednictvím nové soutěže," uvádí ministr pro místní rozvoj **Petr Kulhánek**.

MÍRNĚJŠÍ LEGISLATIVNÍ BYPASS

S ohledem na zajištění právní jistoty úředníků obsahuje návrh také dvě varianty legislativního bypassu – návrh A úplné vypnutí informačních systémů, návrh B částečný bypass spočívající v povinném elektronickém odevzdávání dokumentů a zachování systémů při jejich současném napojením na lokální software dosud používaný stavebními úřady a dotčenými orgány.

„Přiklonili jsme se s kolegy na vládě ke druhé, mírnější variantě. V rámci částečného legislativního bypassu stanoví zákon přechodné období, ve kterém bude činnost v některých informačních systémech stavební správy ze strany stavebních úřadů a dotčených orgánů dobrovolná. Nedojde tedy k vypnutí funkcionalit všech informačních systémů stavební správy, ale k omezení některých evidenčních povinností ze strany stavebních úřadů, pořizovatelů a orgánů územního plánování. Také dojde k rozvolnění náběhu některých funkcionalit informačních systémů," doplnil ministr Kulhánek.

TECHNOLOGICKÝ BYPASS

Z důvodu zvýšení uživatelského komfortu vláda zároveň souhlasila s realizací tzv. technologického bypassu, tedy vybudování rozhraní pro propojení Informačního systému stavebního řízení (ISSŘ), respektive spisové služby DSŘ se systémy, ve kterých stavební úřady vedou řízení zahájená před 30. 6. 2024. Cílem tohoto opatření je automatický přenos výstupů nebo jiných dat mezi ISSŘ (spisovou službou) a externím softwarem.

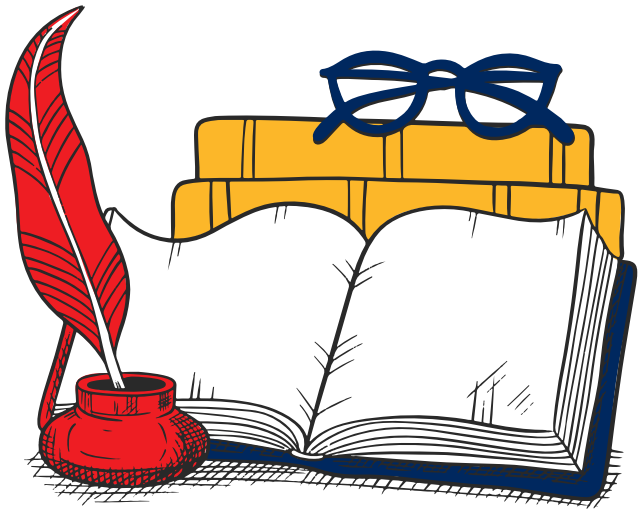
PLNĚ FUNKČNÍ 2028

Ministru pro místní rozvoj vláda tedy uložila iniciovat kroky k realizaci nového zadání veřejné soutěže na zhotovení systému DSŘ ve variantě B: **Nová cesta k cílovému řešení.** To znamená provedení procesní analýzy, vytvoření popisu cílového stavu a nové soutěže na zhotovení systému DSŘ vyjma (NGÚP). K tomu má dojít v otevřeném výběrovém řízení v nadlimitním režimu v hodnotě vyšších stovek milionů korun. Plná funkčnost systémů digitálního stavebního řízení se dá očekávat k 1. 1. 2028, a to včetně potřebného testovacího období. **Do této doby poběží přechodné období.**

LITERÁRNÍ KOUTEK V MIKULOVĚ

Konference v Mikulově zažila již ledacos a v přínosu pro tato překvapení bývá velice aktivní Ministerstvo vnitra. Stálo například u zrodu, kdysi velice populární, volby Miss Egovernment, která na zámku v minulosti probíhala. Roman Vrba, ještě v dresu MV ČR, se zase snažil zavést jakousi sportovní tradici, když při jednom ročníku dokázal vyběhnout na Svatý kopeček a prezentovat odtamtud. Bohužel se z toho kýžená tradice nestala, neboť jsme zjistili, že vyběhnout a nezadýchat se u toho, aby bylo možné prezentovat, nikdo jiný vlastně nedokáže. A letos přišla z řad MV ČR další novinka, jakási předzvěst literárního pojetí prezentací. Možná, pokud se to uchytí, bychom tuto pasáž programu mohli nazývat literárním koutkem Petra Vokáče. Vrchní ředitel sekce legislativy a státní správy MV ČR totiž část svého vystoupení na téma spisových služeb zpracoval do podoby povídky. Natolik se nám líbila, že si ji zde dovolujeme přetisknout.

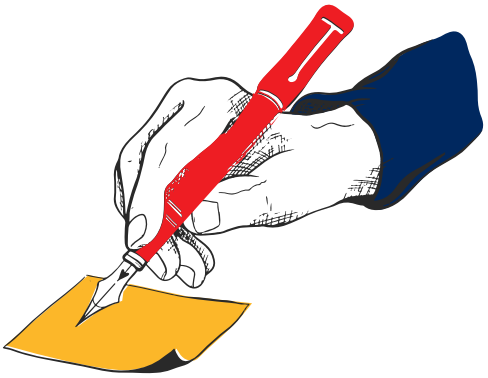
Petr Vokáč uvedl, že chtěl v Mikulově prezentovat především pokroky v nasazení umělé inteligence ve spisové službě. Sice se něco rozběhlo a tak žil v naději, že bude moci prezentovat výsledky **Proof of Concept**, ale vývoj nebyl tak příznivý. Proto si nejprve připravil jen několik jízlivých poznámek, ale nakonec, cestou na konferenci sepsal své postřehy do formy povídky.



JAK JSEM BUDOVAL EGOVERNMENT

Bylo horké léto 2023. Na ministerstvo vnitra dorazil příkaz k úhradě pokuty. Milosrdná lhůta pro podání odporu čítala celé tři kalendářní dny. Není divu, že úřady posílají takováto psaní zpravidla v pátek v poledne. Nebudu vás napínat. Lhůtu jsme propásli. V pátek odpoledne už na úřadě nebylo živáčka, venku pralo slunce, tak se šlo k vodě. Z akce U rybníka jsme pořídili hezkou fotku. Za povšimnutí stojí, že k našemu rybníku občas zavítají i Zajíček s Králíčkem.

Já stál u břehu a jako bývalý odborný náměstek jsem přemítal, nebyla-li chyba, nechat úřad bez odborného dozoru. Když jsem se dozvěděl o pokutě, začal jsem si lámat hlavu, komu takový dohled svěřit? Jak vyřešit práci podatelny tohoto notorického úzkého hrdla? Prozření přišlo až o Vánocích. V čase zbožného usebrání. Zazněl ke mně hlas z nebes.



„Jsem sám starý muž“ pravil, „vím o někom, kdo nespí a k vodě nechodí, protože má tolik parametrů, že se nevejde do plavek“

„To je ono Same Altmane“, zvolal jsem v e-vytržení. Tak se zrodil Proof of Concept použití umělé inteligence v podatelně. Vymyslet to byla hračka. Naučíme velký jazykový model náš organizační řád, budeme mu posílat dokumenty ze spisovky a on je bude vracet i s metadaty a s přidělením vyřizujícímu útvaru. Nyní bylo potřeba nadchnout pro nápad dostatek kolegů. Nadšení pro inovace je ve veřejné správě choroba vzácná, a navíc s dlouhou inkubační dobou. Když se konečně podařilo pár slabších jedinců nakazit, a několik dalších přesvědčit, že by mohlo být dobré chorobu předstírat, tři měsíce byly tytam.

„Vzhůru do práce“ zaveleli jsme unisono s kolegou Hrubým, který na náš úřad přišel nadšením již řádně promořený. Umělá inteligence zpravidla obývá Azzure, takže bylo potřeba vyřešit formulář na kyberbezpečnost.

„Paper Work je moje hobby“, prohlásil jsem sebevědomě a uložil jednomu z kolegů simulantů vyplnit formulář podle vyhlášky 82. Ať se snažil, jak chtěl, pořád mu to ale nevycházelo. „Pane vrchní, ve spisovce jsou dvě stížnosti, kde se píše, že jste slabomyslný. To je citlivý osobní údaj, a tedy kritické aktivum. Do Azzure nás to nepustí.“

„Uhni, škarohlíde,“ zavelel jsem. „Budeme se muset zamyslet.“

Škoda, že jsme se nezamysleli o měsíc dřív. Byli bychom už tehdy zjistili, že potřebujeme vyplnit formulář podle vyhlášky 315.

„Vezmi to zpět a piš znovu“ pokynul jsem kolegovi. Obrátil se na mě plachým pohledem laně s otázkou „jak se to bere zpátky?“ a tady jsem mohl ukázat, že jsem na gymnáziu nechodil na informatiku nadarmo. „Podívej se nahoru na lištu, zmáčkni to tlačítko s popisem Undo!“ Kolega si myslel, že mu sprostě nadávám, urazil se a odešel středem.

Nezbylo, než abych si s Undem poradil sám. Když jsem konečně vyplnil formulář, kde po kritické úrovni nebylo ani památky, vítězně jsem vtrhnul do kanceláře kolegy Hrubého. „Máme to, můžeme to spustit,“ jásal jsem jako septimán po debuggingu. Z oblaku dýmu se ozvalo temné zavrčení: „nemůžeme, nemáme Azzure.“

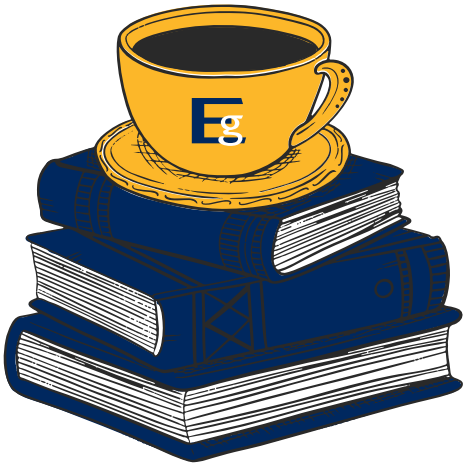
„Cože nemáme Azzure? Jak si to mohl dopustit? Tomáši, ty, profesionál, průkopník, přítel.“

„No, na tohle jsem krátkej,“ odvětil. „Na finančním oddělení mají dovolenou.“

„Ale takhle to nebudu moc prezentovat v Mikulově,“ rval jsem si vlasy. Když kolega Hrubý shledal mé zoufalství, přispěchal s východiskem. „Budeš to muset nějak okecat. To ty zvládneš, věřím ti.“

Ramena se mi prohnula pod tíhou nečekané výzvy.

„Ale neboj,“ dodal kolega útěšně, „ v Mikulově se to zlomí, tam je azuro furt.“



„Pravda“ přitakal jsem, „ale Tomáši, také se tam značně zamlžuje úsudek.“

„No právě, tam zase vymyslíme projektů.“

Náhlá vlna optimismu nás dojala. Že ve státní správě všechno trvá? Že máme složitá pravidla veřejných zakázek? A když je něco jednoduché, tak si to aktivně zesložitíme? Že neumíme zaplatit odborníky? Že dřív, než zavedeme umělou inteligenci do spisovky, uzná Sam Altman, že jazykové modely nemají duši? Nevadí. Nemít srdce vadí.

Zahleděli jsme se ke vzdálenému obzoru, povzdychnul jsem si, „S námi srdcaři čeká eGgovernment skvělá budoucnost.“

Pokud si povídku chcete poslechnout v podání samotného autora, najdete ji v rámci videozáznamu vystoupení Petra Vokáče na konferenci v Mikulově.

NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI: PREVENCE JE VŽDY LEPŠÍ A LEVNĚJŠÍ

Návrh nového zákona o kybernetické bezpečnosti byl 17. července schválen vládou a postoupen Poslanecké sněmovně. V průběhu prvního čtení zazněly 17. září v Poslanecké sněmovně opět argumenty, které opakovaně zaznívaly i během všech předešlých přípravných fází. Bylo odhlasováno, že se návrhem zákona bude podrobněji zabývat výbor pro bezpečnost, a dále hospodářský výbor a výbor pro obranu.

Hlavním argumentem proti návrhu zákona je jeho široká působnost, respektive vysoký počet regulovaných subjektů. S tím souvisí administrativní zátěž regulovaných organizací, hlavně pak zátěž obcí s rozšířenou působností, které mají do navrhovaného regulatorního rámce nově také spadat. Specificky tzv. mechanismu bezpečnosti dodavatelských řetězců je vytýkáno, že nebyl dostatečně probrán, že nebyly zohledněny vznesené připomínky, a v obecnější rovině, že by o takových věcech měla rozhodovat vláda.

Účelem dalšího textu není obhajoba vůči dílčím námitkám vzneseným v průběhu dosavadního legislativního procesu, ale vysvětlení potřebnosti a nezbytnosti nového přístupu pro zajišťování kybernetické bezpečnosti v České republice. Lidsky řečeno, pojďme se podívat na to, k čemu má nový zákon o kybernetické bezpečnost vést a na co konkrétně reaguje.

Směrnice NIS2 je minimální požadavek Unie

Prvotní návrh zákona vznikl již v lednu roku 2023, tedy nedlouho potom, co nabyla účinnosti tzv. směrnice NIS2, kterou návrh zákona transponuje do českého právního řádu. Tento evropský předpis používá metodu tzv. minimální harmonizace, tedy že členský stát musí splnit minimální požadavky stanovené směrnicí. Nemůže si stanovit užší působnost regulace. Nemůže regulovaným organizacím uložit méně povinností. Nelze se rozhodnout, že některá část směrnice nebude transponována a používána v národním právním řádu. Pokud by se tak stalo, hrozí zde sankce ze strany Evropské komise za nesprávnou transpozici.

Národní úřad pro kybernetickou a informační bezpečnost se rozhodl pro zachování maximální transparentnosti a dobrovolně vyhlásil veřejnou konzultaci, během které mohl kdokoliv uplatnit své připomínky, návrhy a podněty. Řada připomínek uplatněných již v průběhu veřejných konzultací směřovala přímo proti požadavkům směrnice NIS2. Vyhovění těmto připomínkám by znamenalo nesprávnou transpozici a riziko sankcí. Přesto řada z těchto výtek přetrvává až do aktuálně probíhajících fází legislativního procesu.

Racionalizace a přizpůsobení se ekonomické realitě

Přes výše zmíněné se NÚKIB snaží reflektovat ekonomickou realitu a zmírňovat v rámci zákonných mezí dopady směrnice NIS2. Nikdo si nepřeje zbytečně zatěžovat malé podniky nesmyslně extenzivními povinnostmi v jakékoliv oblasti, nejen v kyberbezpečnosti. Veškeré povinnosti pro poskytovatele v tzv. nižším režimu povinností by

měly směřovat k zavedení minimálního bezpečnostního standardu, tedy sady nejzákladnějších bezpečnostních opatření.

Zavedením základních bezpečnostních opatření chrání daná organizace především sama sebe a svůj „byznys“. V minulých letech se projevovala tendence banalizovat požadavky GDPR, jehož účelem je primárně ochrana práv osob, jejichž údaje jsou zpracovávány. Správci údajů často považovali za zbytečné vynakládat finanční prostředky na ochranu práv a zájmů někoho jiného. Soulad s GDPR se často řešil hlavně z důvodu potenciálně vysokých sankcí, případně z reputačních důvodů.

Nezaváděním kyberbezpečnostních opatření však organizace ohrožují své vlastní fungování. Přístup „koupím štos dokumentace a nestarám se“, kterým se řada organizací vypořádala s GDPR, nebude v oblasti kyberbezpečnosti fungovat. Tímto způsobem nedojde k ošetření rizik a k zabezpečení organizace. Takový přístup není racionální, ekonomicky ani nijak jinak, a vysvětlíme si proč.

Přístup založený na řízení rizik v běžném životě

Většině lidí přijde zcela normální, že zamknou dveře, když odchází z domu. Používáme bezpečnostní pásy, když jedeme v autě. Na kole zpravidla používáme helmu, zvlášť když víme, že pojedeme po frekventovanější silnici. Automaticky vyhodnocujeme rizika a hrozby okolo nás, reagujeme na ně a snažíme se vyhnout nepříznivým dopadům na naše zdraví či majetek.

Bylo by vhodné se obdobně obezřetným způsobem chovat také v kyberprostoru, ale dlouhodobě se ukazuje, že jsou hrozby a rizika v kyberprostoru podceňovány navzdory tomu, že se významná část našich životů přesunula do online prostředí. Vrátíme-li se k původnímu přirovnání, nechávají se otevřené dveře od domu, protože si říkáme, že náš dům přece pro zloděje nemůže vypadat nijak lákavě.

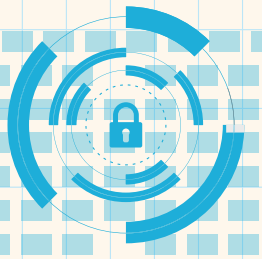
Útoky v kyberprostoru jsou často plošné a necílené. Útočník má možnost, často z důvodu slabé bezpečnosti, nahlížet do nespočtu otevřených dveří, bez ohledu na to, jak velká či důležitá daná organizace je. Tvrdíme-li, že kybernetická bezpečnost má být problematikou pouze pro pár vyvolených organizací ve státě, je to srovnatelné s tvrzením, že si dům mají zamykat pouze bohatí lidé a pásy v autě používat pouze rallye závodníci.

Prevence je vždy lepší a levnější

Hlavním účelem nového zákona má být osvěta vedoucí ke změně uvažování o rizicích s původem v kyberprostoru. Směrnice NIS2 ani nový zákon nedopadají plošně na všechny organizace v České republice, ani neukládají žádné povinnosti jednotlivcům. Podniky splňující velikostní kritéria a poskytující své služby v zákonem specifikovaných odvětvích však musí začít reflektovat realitu, tedy exponenciální nárůst kybernetických útoků.

Nabízí se námitka, že k osvětě není zapotřebí žádná nová regulace. Z praxe však vyplývá, že neregulovaná organizace začne zpravidla řešit kyberbezpečnost až ve chvíli, kdy se sama stane cílem útoku – to je pozdě a je to zbytečně drahé. Ukazuje se, že bez právní povinnosti a sankce je posun v úrovni kyberbezpečnosti velmi malý či nulový. Stav zabezpečení organizace často záleží pouze na iniciativě uvědomělých správců IT v dané organizaci a jejich schopnosti a vůli přesvědčit vedení o důležitosti tohoto tématu a výhodnosti investic do bezpečnosti, oproti nákladům na řešení dopadů incidentů.

Zavedení alespoň základních bezpečnostních opatření může snížit šance na úspěšný útok o 30 až 50 %. O tom, co jsou základní bezpečnostní opatření, co je tak zvaně *must have*, nebo naopak *nice to have*, se povedou debaty v rámci mezirezortního připomínkového řízení k vyhláškám o bezpečnostních opatřeních. O tom, že by kybernetickou bezpečnost v rozumné a přiměřené míře měl řešit každý, o tom již debatovat nemusíme. Vždy je lepší být připraven, než překvapen.



Štěpán Daněk
Oddělení regulace veřejného sektoru
Národní úřad pro kybernetickou
a informační bezpečnost
Gorkého 10, 602 00 Brno
mobil: +420 702 146 218
e-mail: stepan.danek@nukib.gov.cz
https://nukib.gov.cz

KVALIFIKOVANÍ A NEKVALIFIKOVANÍ POSKYTOVATELÉ SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Revize nařízení eIDAS[1], často označovaná jako eIDAS 2.0, je spojena především s Evropskou peněženkou digitální identity (EDIW). Stranou pozornosti by však neměly zůstat další změny, včetně stanovení požadavků na nekvalifikované poskytovatele služeb vytvářejících důvěru (čl. 19a). Pokud jde o typy služeb, může nekvalifikovaný poskytovatel nabízet totožné služby jako kvalifikovaný, pouze výstupy – certifikáty, časová razítka a služby s nimi související – nemohou nést označení „kvalifikovaný".

Na konkrétním příkladu je možné ukázat rozdíl – nařízení eIDAS v původní i revidované verzi stanoví, že pouze:

- kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu;
- kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

Při rozhodování, zda použít služby kvalifikovaného, nebo nekvalifikovaného poskytovatele, je nutné vzít v úvahu i požadavky národní legislativy. Ve zkratce – u nás platí, že při komunikaci, kdy nejméně jedním z komunikujících je orgán veřejné moci a kdy se jedná o úkon či právní jednání, je nutné použít kvalifikovaný certifikát.

Pokud se jedná o odpovědnost za škodu a důkazní břemeno, požadavky zůstávají v revidovaném eIDAS stejné. Důkazní břemeno, pokud jde o úmysl nebo nedbalost nekvalifikovaného poskytovatele služeb vytvářejících důvěru, nese fyzická nebo právnická osoba uplatňující nárok na náhradu škody. V případě kvalifikovaného poskytovatele služeb vytvářejících důvěru je to naopak, úmysl nebo nedbalost se předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že újma nastala bez jeho úmyslu nebo nedbalosti. Ve zkratce – v případě nekvalifikovaného poskytovatele musí ten, kdo se od něj domáhá náhrady škody, předložit důkaz o pochybení sám, a to může být poměrně obtížné. Kvalifikovaný poskytovatel naopak musí sám předložit důkaz, že ve smyslu eIDAS nepochybil.

Je možné zmínit další odlišnosti v požadavcích na kvalifikované a nekvalifikované poskytovatele. Kvalifikovaní

[1] Nařízení Evropského parlamentu, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu. Dostupné na https://eur-lex.europa.eu/

musí před zahájením poskytování služby oznámit orgánu dohledu svůj úmysl spolu s předložením zprávy o posouzení shody vydanou subjektem posuzování shody, která potvrzuje splnění všech stanovených požadavků. Do celkového posuzování může být zapojen i subjekt s kompetencí posuzování splnění požadavků podle směrnice NIS2. Teprve pak může být udělen kvalifikovaný statut. Následně se kvalifikovaný poskytovatel musí na vlastní náklady alespoň jednou za 24 měsíců podrobit auditu ze strany subjektu posuzování shody a zprávu předložit orgánu dohledu. O plánovaných auditech musí informovat dohledový orgán předem a umožnit mu účast při jejich provedení. Nad tento rámec se musí podrobit auditu kdykoliv si to orgán dohledu vyžádá, a to na vlastní náklady. Naopak nekvalifikovaný poskytovatel svůj úmysl neohlašuje, povinnost pravidelných auditů se na něj nevztahuje a orgán dohledu vykoná kontrolní akci jen v odůvodněných případech, nikoliv pouze z vlastní iniciativy.

Pokud jde o rozhodování, zda se stát kvalifikovaným či nekvalifikovaným poskytovatelem, může sehrát negativní roli skutečnost, že revidované znění eIDAS stanoví, že „do 21. května 2025(sic!) stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy“ vztahující se k nekvalifikovaným poskytovatelům. Oba typy poskytovatelů tedy nebudou muset plnit stejné normy, resp. stejný rozsah norem.

Ještě méně jasno je ve vztahu ke směrnici NIS2, tj. celoevropské směrnici o kybernetické bezpečnosti. Jisté je, že se vztahuje na oba typy poskytovatelů. Návrh prováděcího předpisu nerozlišuje kvalifikované a nekvalifikované poskytovatele, pro všechny stanoví stejné povinnosti. Naskýtá se otázka, proč nedat přednost tomu působit jako kvalifikovaný poskytovatel. Samozřejmě bezpečnost vždy něco stojí a budou-li mít nekvalifikovaní poskytovatelé stejné povinnosti a budou tedy nuceni vynaložit stejné prostředky pro jejich naplnění, ztratí i jednu z mála výhod – jejich služby bývají pro uživatele o něco levnější. Z hlediska kvalifikovaných poskytovatelů se zesílí dohled, kromě orgánu dohledu nad kvalifikovanými poskytovateli bude uplatněn i dohled stanovený NIS2. V našich podmínkách to budou Digitální a informační agentura (jako dosud) a nově rovněž NUKIB.

Pojem „nekvalifikovaný“ by však neměl evokovat představu, že poskytovatel nedosáhl potřebné kvalifikace či úrovně, je tedy „méně dobrý“, sportovní terminologií nekvalifikoval se. Tak tomu není, poskytovatel se sám rozhoduje, zda má v úmyslu – a odpovídá to jeho obchodním zájmům – stát se kvalifikovaným. Může například poskytovat služby takovému segmentu trhu, kde kvalifikované služby nejsou vyžadovány. A jak se potenciální zájemce dozví, zda se jedná o kvalifikovaného poskytovatele/kvalifikovanou službu? V každém případě z jeho Certifikační politiky, v případě kvalifikovaných pak ze seznamu, který zveřejňuje DIA, a webových stránek EK nazvaných eIDAS Dashboard. Nekvalifikovaní poskytovatelé v těchto seznamech být mohou, ale nemusí. Kvalifikovaní mohou používat tzv. značku důvěry, s platností v celé EU.
Závěrem je možné citovat z webových stránek Evropské komise: „Z právního hlediska mají kvalifikované i nekvalifikované služby vytvářející důvěru výhodu z nediskriminační doložky jako důkazu u soudů. Jinými slovy, služby vytvářející důvěru nelze v soudním řízení odmítnout pouze na základě toho, že jsou v elektronické podobě, nebo proto, že nejsou kvalifikované.

Vzhledem k přísnějším požadavkům na kvalifikované poskytovatele služeb vytvářejících důvěru však mají kvalifikované služby silnější konkrétní právní účinek než nekvalifikované, a také vyšší technické zabezpečení. Kvalifikovaný elektronický podpis má stejný právní účinek jako vlastnoručně psaný podpis. U kvalifikované elektronické pečeti platí presumpce integrity dat a správnosti původu těch dat, ke kterým je kvalifikovaná elektronická pečeť připojena. Kvalifikované elektronické potvrzení atributů a elektronické potvrzení atributů vydané orgánem veřejného sektoru odpovědným za autentický zdroj, nebo jeho jménem, má stejný právní účinek jako zákonně vydané potvrzení v listinné podobě. Kvalifikované služby tak poskytují vyšší právní jistotu a vyšší bezpečnost elektronických transakcí.“

Dagmar Bosáková
První certifikační autorita, a.s.

NÁVRAT DO KANCELÁŘÍ, NEBO HOME OFFICE?

Blíží se výročí pěti let od vypuknutí covidové pandemie, která, kromě jiného, celosvětově rozšířila hybridní model práce. Komunikační technologie, které byly do té doby doménou IT společností, najednou objevil a začal používat celý svět. Původní všeobecná euforie již vyprchala a nadešel čas nové uspořádání práce hodnotit střízlivě.

Po pěti letech je zcela zřejmé, že zaměstnanci se zpět do kanceláří nevrátí, alespoň ne v té míře, jako tomu bylo před pandemií. Zatímco v roce 2019 pracovalo z domova dle studie think tanku IDEA pouze 10 % Čechů, v době koronavirové pandemie vzrostl tento podíl až na 40 % a v současné době je to více než pětina zaměstnanců. K nejčastějším oborům patří logicky nevýrobní segmenty: například IT, finance, marketing, zdravotnictví nebo personalistika.

Neotřesitelná pozice modelu hybridní práce je tak evidentní, že možnost pracovat z domova se postupně v nabídkách práce ztratila z pozice nabízených firemních benefitů. Home office už prostě nezaujímá místo benefitu vedle multisport karty nebo příspěvku na penzijní připojištění, ale stal se samozřejmostí. Hraje mimořádně důležitou roli v rozhodování lidí při výběru zaměstnání. Například podle průzkumu poradenské společnosti McKinsey zaujímá možnost hybridní práce třetí příčku při rozhodování o volbě zaměstnání. Hned za výší platu a možností kariérního růstu.

HYBRIDNÍ VEŘEJNÁ SPRÁVA?

Existuje řada příležitostí, při nichž i výkon funkcí veřejné správy může probíhat hybridně a velmi efektivně. Nedávné povodně na Moravě a v jižních Čechách mohou posloužit jako vzorový příklad. Kdy jindy by měli být například pracovníci Úřadu práce, sociálních služeb, statici a další přímo v terénu, u postižených lidí. Jako příklad využití digitálních komunikačních nástrojů v „dobách míru" může posloužit více než čtyřicítka policejních PolPointů. Na vybraných místech mohou občané prostřednictvím videokonferenčního zařízení například oznámit trestný čin, aniž by museli navštívit policejní úřadovnu.

15 LET ZKUŠENOSTÍ CISCO

Pro lidi v Ciscu nebyla práce na home office žádné novum ani před covidem. Jednalo se a stále se jedná o zcela běžně používaný model. Cisco dlouhé roky vyvíjí technologie pro videokonference a s platformou Webex pracuje již od roku 2007. *„Jde o model, který je hluboko zažitý v DNA firmy. Když přišel covid, nastoupili zaměstnanci na home office prakticky ze 100 %, po jeho odeznění se*

vrátili k našemu normálu. To znamená, že zhruba 50 % zaměstnanců Cisco v ČR pracuje na home office. Samozřejmě je to rozdílné u různých profesí. Například obchod je do značné míry týmovou prací, takže u něj je více lidí v kanceláři. Ale třeba i vývojáři v našem R&D centru hodně věcí vymýšlejí společně. Naopak třeba lidé v regionálních pozicích pro Evropu pracují více jako vzdáleně připojení," popisuje generální ředitelka Cisco ČR Zuzana Švecová.

ZAMĚSTNANCI PRÁCI NA DÁLKU MILUJÍ

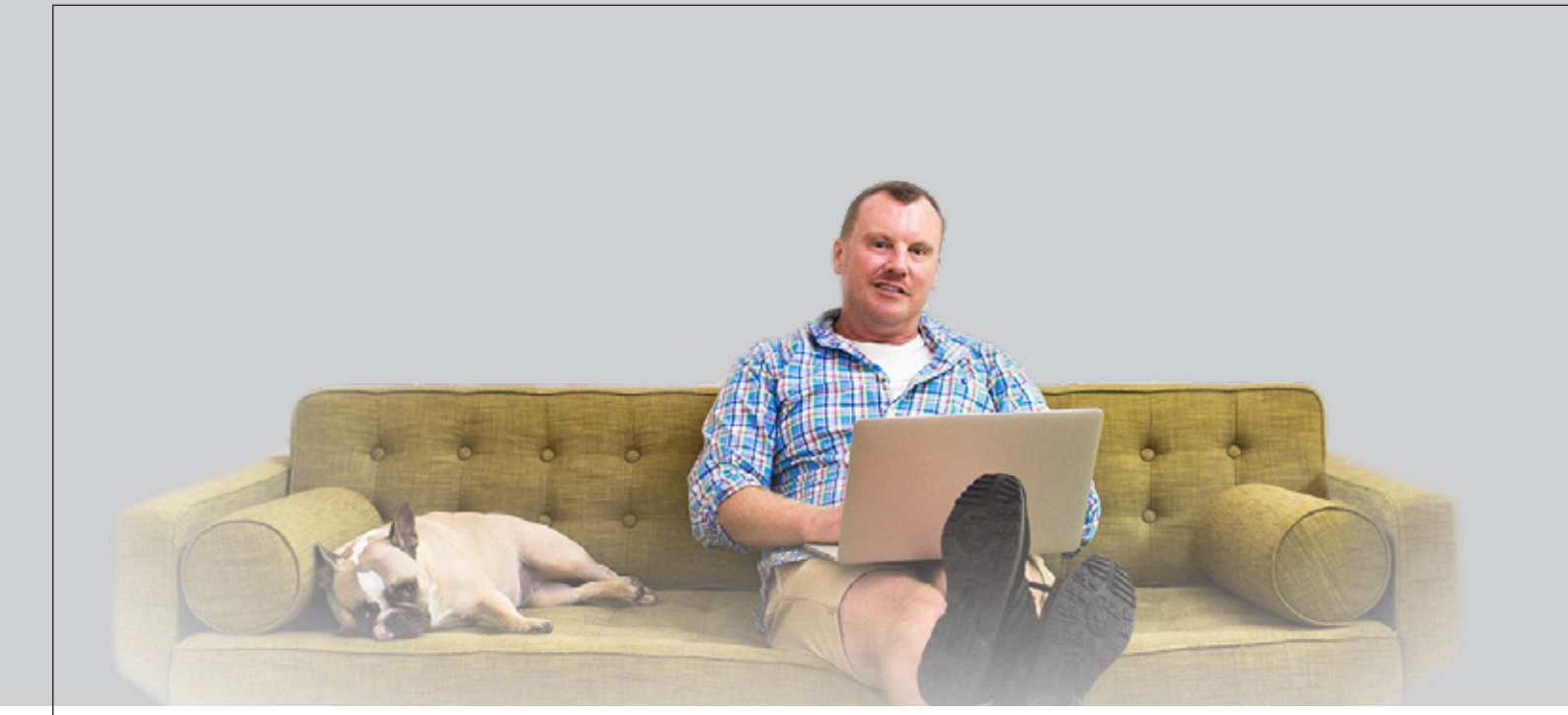
Výhody modelu hybridní práce pro zaměstnance jsou evidentní – možnost flexibilně si uspořádat pracovní dobu v průběhu dne, úspora času a financí spojených s dojížděním do zaměstnání. V českých podmínkách to asi ještě nikdo nespočítal, ale v globálním výzkumu Cisco vyčíslili týdenní úspory na benzínu, jízdném či stravování na 150 dolarů! Podle stejného zdroje šetří téměř dvě třetiny respondentů při práci z domova čtyři hodiny týdně, a více než čtvrtina dotázaných dokonce osm a více hodin týdně, strávených v autě, autobuse nebo vlaku. K těm „měkčím", ale mnohdy docela zásadním, benefitům patří soukromí a klid na práci. Při práci v open office se totiž mnoho lidí jednoduše nemůže plně soustředit. Více než polovina zaměstnanců tvrdí, že hybridní práce jim pomohla snížit úroveň stresu a více než 80 % dotázaných dokonce prohlašuje, že jsou díky možnosti pracovat odkudkoli šťastnější!

Ve výčtu subjektivních pozitivních dojmů na straně zaměstnanců by se dalo pokračovat, ale zdaleka to není jen růžové. Hodně zaměstnanců se třeba obává, že práce na dálku může mít negativní dopady na jejich finanční oceňování a kariérní postup, v duchu hesla „sejde z očí, sejde z mysli". Statistiky Forbes Advisor uvádějí, že téměř 70 % pracovníků zažilo pocit vyhoření právě v důsledku přemíry digitální komunikace.

MANAŽERSKÁ PARANOIA

Firemní pohled na home office už není zdaleka tak jednoznačný. Benefity jsou i v tomto případě nasnadě: menší počet lidí v kancelářích znamená úspory elektřiny a dalších energií, v nákladech na úklid nebo nižší nároky na parkovací místa. Zatímco manažeři tvrdá data o finančních úsporách vidí na první pohled, neplatí totéž o výkonnosti pracovníků, kteří se „rozutekli" do svých domovů. Tahle situace dokonce nabývá až paranoidní podobu: zatímco zaměstnanci svorně ve všech průzkumech tvrdí, že jsou při práci z domova stejně, nebo i více produktivní, skoro 90 % lídrů prohlašuje, že nemají plný přehled o produktivitě svých podřízených. Manažerská nejistota a nervozita je bezesporu i jedním ze zdrojů častého volání po „návratu do kanceláří".

Generální ředitelka Cisco ČR Zuzana Švecová a Cisco Collaboration Specialist Jaroslav Martan



HOME OFFICE NEBO KANCELÁŘ?

Na otázku, jaké prostředí je efektivnější či produktivnější, zda pohodlí domova, nebo kancelář, v současné době asi neexistuje jediná správná odpověď. Pravda bude někde uprostřed. Například průzkum Stanford University tvrdí, že 2 až 3 dny práce z domova v týdnu nemají žádný negativní vliv na firemní kulturu, produktivitu či inovace.

V Ciscu myslíme na dvě zásady:

- Pokud chcete, aby se lidé alespoň částečně vraceli do kanceláří, musíte jim k tomu dát důvod. Tou největší motivací mohou být kontakty s dobrými kolegy a kamarády. Dalším dobrým důvodem může být perfektně vybavené prostředí pro práci a komunikaci vícečlenných týmů. Zároveň ale i kancelářské prostory musí nabídnout takové prostředí, kde je zajištěno absolutní soukromí.
- Pokud chcete podporovat produktivitu lidí na home office, musíte jim pomoci vytvořit stejné uživatelské prostředí jako v kanceláři.

ČESKÁ NERADOSTNÁ REALITA

Na téma přístupu českých firem k vybavení zaměstnanců, kteří pracují částečně nebo zcela z domova, Cisco provedlo před časem rozsáhlý průzkum. Ten odhalil technologické rezervy ve třech oblastech: v technickém vybavení a dostupných službách při práci z domova, v zabezpečení dat a v podpoře vzdálených uživatelů.

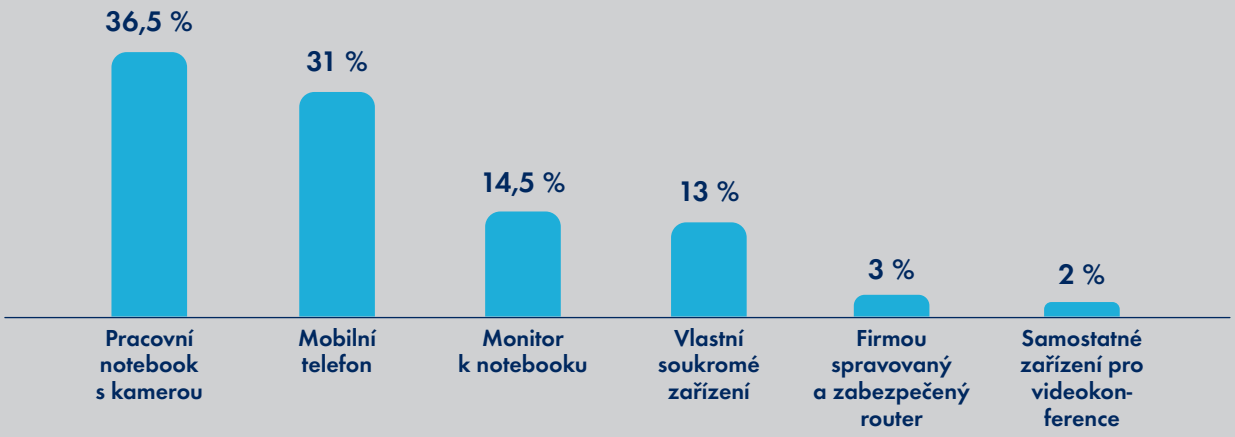
„V kanceláři jsou uživatelé už dnes často zvyklí na to, že mají před sebou velký monitor nebo personální videokonferenční zařízení s potřebnou ergonomií, a vedle třeba komunikačně vybavenou zasedačku s intuitivní obsluhou. Doma lidem tenhle základní komfort běžně chybí a musí se krčit u notebooku s kamerkou několik hodin denně. Trpí tím pak nejenom tělo z pohledu ergonomie a následně zdraví, ale především i všichni vzájemně komunikující z hlediska uživatelského zážitku a výsledné produktivity takovýchto schůzek. Podle výsledků našeho průzkumu jen zhruba 2 % firem dala svým zaměstnancům samostatné zařízení pro videokonference," vysvětluje Cisco Collaboration Specialist Jaroslav Martan.

RADA ODBORNÍKA

„Jako distributor nástrojů pro spolupráci Cisco vidíme vzrůstající poptávku po těchto řešeních ve veřejné správě. Zaměstnanci úřadů a institucí potřebují mít možnost vyřizovat pracovní věci, i když nesedí u svého pracovního stolu. Nástroje Cisco jsou pro tento účel vhodné díky propracovanému zabezpečení, které pomáhá chránit data úřadů i občanů."

ALEF

VYBAVENÍ ZAMĚSTNANCŮ PRO HYBRIDNÍ PRÁCI



Důležitou (a podceňovanou) oblastí je také podpora vzdálených uživatelů. Pokud pracovníkovi na home office přestane fungovat připojení, IT podpora jeho firmy obvykle jen těžko odhalí přesnou příčinu problému, které může být v neaktualizovaném domácím wi-fi routeru, u poskytovatele připojení nebo kdekoliv na trase. Firemním IT specialistům by tak výrazně usnadnily život nástroje, které umí monitorovat kvalitu připojení a dostupnost firemních služeb bez ohledu na lokaci uživatele. V českých podmínkách ale jen asi třetina firem dokáže poskytnout vzdáleným pracovníkům podporu a diagnostikovat vzniklé problémy „end-to-end" od zařízení uživatele až do firemní sítě.

DÍRY V BEZPEČNOSTI

Samostatnou kapitolu pak představuje zabezpečení hybridního prostředí. Z českého průzkumu Cisco vyplynulo, že plná pětina firem vůbec NEVÍ, zda v souvislosti s hybridní prací čelily útoku či nikoliv. Firmy přitom mají podle průzkumu i technologické rezervy ve způsobu, jakým dovolí vzdáleným pracovníkům přistupovat k datům a aplikacím. Jen u 32 % společností vyžadují firemní aplikace přístup přes virtuální privátní síť (VPN) a jen u přibližně pětiny společností se pro vstup k firemnímu IT používá vícefaktorová autentizace. Zhruba 20 % vyžaduje, aby veškerá komunikace vzdáleného pracovníka po internetu probíhala přes VPN a firemní firewall.

Velkým problémem je, že se v modelu hybridní práce částečně nebo zcela stírají hranice mezi soukromým a firemním. Soukromá a firmou nespravovaná zařízení totiž představují stále častější vektor hackerských útoků. Nejnovější průzkum Cisco Cybersecurity Readiness Index poukázal na obří rozsah tohoto problému, neboť 85 % společností v něm uvedlo, že jejich zaměstnanci přistupují k firemním platformám z nespravovaných zařízení. A 43 % těchto pracovníků tráví pětinu svého času na svém soukromém notebooku právě ve firemních sítích. To už je pro hackery docela velké pole působnosti!

Hybridní model se stal integrální součástí pracovního prostředí v mnoha profesích. Došlo by k tomu i bez covidové pandemie, která přechod k němu jen urychlila. Firmy by měly svým pracovníkům vytvořit takové technologické podmínky, aby mohli z domova pracovat stejně jako v kanceláři. A současně podporovat takové prostředí a atmosféru v kancelářích, aby se do nich zaměstnanci rádi vraceli.

-red-

GORDIC PŘEDSTAVIL AKTUÁLNÍ TRENDY V IS VEŘEJNÉ SPRÁVY

Mikulov opět hostil další ročník vyhledávané konference E-governmentu, v pořadí již šestnáctý. O oblíbenosti konference svědčí fakt, že na ni letos zavítala téměř tisícovka návštěvníků. Záštitu nad konferencí převzal Ivan Bartoš, místopředseda vlády pro digitalizaci a ministr pro místní rozvoj, Martin Kupka, ministr dopravy, Jan Grolich, hejtman Jihomoravského kraje, a Jitka Sobotková, starostka Mikulova. Generálním partnerem se opět stala společnost Gordic.

V odpoledním bloku seznámili zástupci firmy Gordic, Michal Tausch, ředitel odboru podpory obchodu, a Michal Polák, vedoucí oddělení vývoje aplikačního SW, všechny účastníky s aktuálními trendy v informačních systémech veřejné správy. Mezi hlavní body jejich prezentace patřila aplikace zákona o právu na digitální služby, AI ve veřejné správě, cloud computing, elektronická spisová služba a implementace směrnice NIS2.

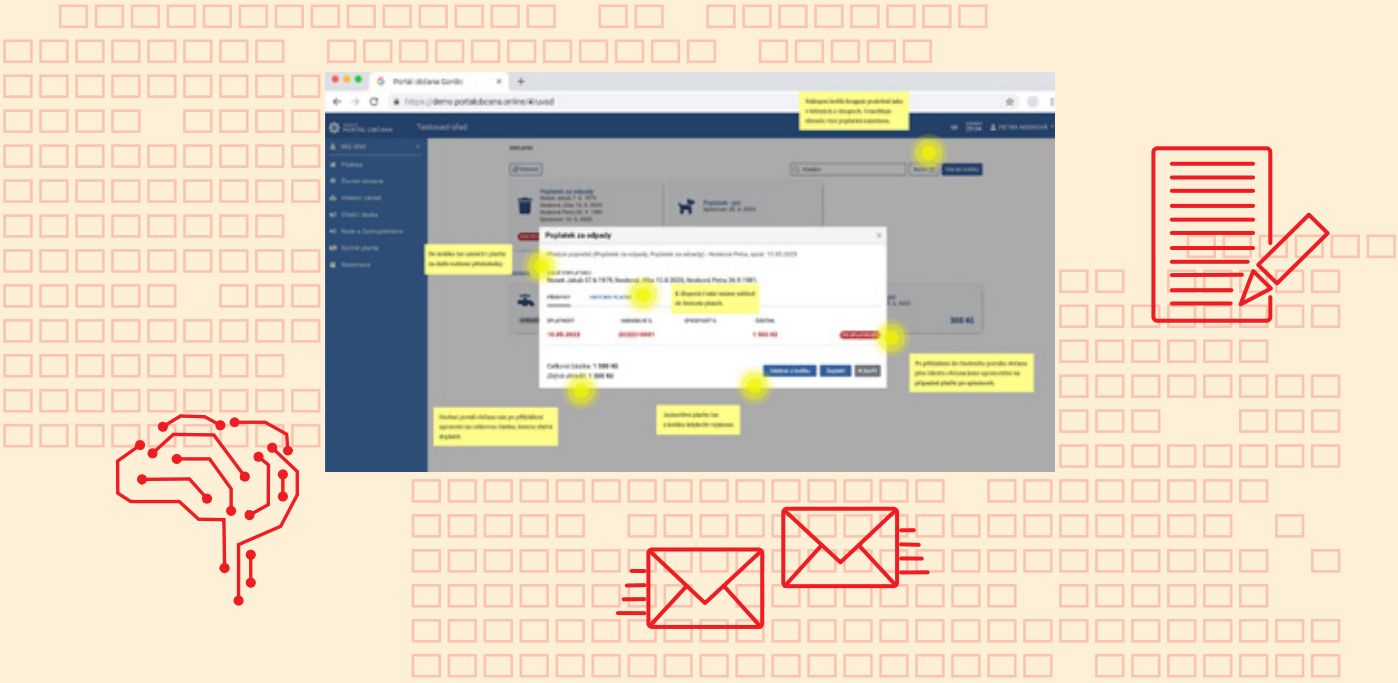
Digitální služby: nezůstat v půli cesty

„Kdo se zúčastnil dopolední části konference, určitě slyšel, že se toho v oblasti digitálních služeb státní správy stalo hodně. Zásadní je ale nezůstat v půli cesty. Je skvělé, že existují nějaké digitální formuláře, které můžeme online vyplnit, ale tím to samozřejmě nesmí skončit," řekl v úvodu prezentace **Michal Tausch**.

Podle něj by neměl po vyplnění následovat export dat a nutnost je odeslat datovou schránkou nebo prostřednictvím e-mailů. *„Digitální služba musí být dostupná prostřednictvím samoobslužných portálů s jednotným přihlášením prostřednictvím autentizace. Samozřejmostí by mělo být i předvyplňování údajů, které mají úřady k dispozici díky napojení na registry. V neposlední řadě musí v těchto samoobslužných portálech existovat možnost odeslání nebo úplného elektronického podání,"* pokračoval **Michal Tausch**.

Společně s **Michalem Polákem** návštěvníkům představili nové funkcionality, které nabízí Osobní portál občana od společnosti Gordic – jednodušší zastupování a nákupní košík. Funkce portálu občana nazývaná „mandát/y" umožní jednat v zastoupení za fyzickou či právnickou osobu. Člověk tak na základě mandátu může například učinit elektronické podání za společnost.

Další novinkou je nákupní košík, který umožňuje úhradu více poplatků najednou. Příkladem je košík v běžných e-shopech, který v případě Osobního portálu občana funguje obdobně. Stačí se přihlásit do portálu přes Identitu občana a okamžitě vidíte poplatky k uhrazení. Vybranou položku pak vložíte do košíku a uhradíte pomocí platební brány.



Vytěžování faktur pomocí AI

Prezentace společnosti Gordic se dotkla i tématu AI ve veřejné správě. *„Díky integraci s řešením NATHAN od společnosti Multima společnost Gordic přináší do IS GINIS další způsob využití umělé inteligence, která pomůže efektivně vytěžit data z faktur a účtenek. Dokáže tak s vysokou spolehlivostí rozpoznat data z různých typů dokumentů – od obrázku až po PDF. Vytěžená data se automaticky zobrazí vedle detailů faktury, kde je možné je snadno zkontrolovat a upravit,"* vysvětlil při praktické ukázce **Michal Polák**. Trendem, který byl v prezentaci zmíněn, je cloud computing. Naše nabídka SaaS služeb byla zapsána do Katalogu cloud computingu. Patříme tak mezi firmy, které jsou uznány jako způsobilé pro poskytnutí cloudových služeb z hlediska své bezúhonnosti a zajištění dodržování práv třetích osob. Každá z firem musí před zápisem projít náročným administrativním procesem, splnit zadaná bezpečnostní kritéria, tak aby byla schopna zajistit požadovanou úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánů veřejné správy.

Snazší schvalování a podepisování

Atestace elektronických spisových služeb jsou sice odloženy, ale ani tak vývoj v této oblasti nespí. Novinkou, kterou řečníci představili, byl Manažerský semafor. Jedná se o rozšíření online aplikace Elektronická podpisová kniha (EPK) a slouží k označování dokumentů podle jejich rizikovosti. Asi každý manažer ví, že administrativa a podepisování dokumentů může být neúprosná rutina, která následuje za každodenními pracovními úkoly. Tento nástroj je určený zejména pro manažery a vedoucí pracovníky, kteří se potýkají s velkým objemem dokumentů připravených ke schvalování a podepisování. Využívat ho mohou všechny typy organizací. Celý nástroj je povýšen prostřednictvím integrace na řešení společnosti Software602, který kromě dalších prvků umožňuje i hromadné schvalování a podepisování kvalifikovaným podpisem.

Analýza kybernetické bezpečnosti je cestou ke splnění požadavků NIS2

V závěru prezentace se přednášející věnovali tématu nové evropské směrnice NIS2, která přináší rozsáhlé změny a nové povinnosti pro firmy a veřejné instituce v České republice. Aktualizovaná verze původní směrnice NIS si klade za cíl posílit ochranu kybernetické infrastruktury před rostoucím nebezpečím kybernetických útoků. Pomoci může specializovaná aplikace GORDIC CSA (CyberSecurity Audit), která umožňuje tzv. audit kybernetické bezpečnosti snadno zpracovat a zajistí celkové procesní řízení kybernetické bezpečnosti.

GORDIC

watsonx.governance

WATSONX.AI: GENERATIVNÍ UMĚLÁ INTELIGENCE, KTERÁ JE PŘIZPŮSOBENA VAŠÍM POTŘEBÁM

Podle nedávné studie IBM Institutu for Business Value čelí až 64 procent dotázaných generálních ředitelů tlaku na urychlení zavádění generativní umělé inteligence a 60 procent z nich postrádá konzistentní celopodnikovou metodu pro její implementaci. Umělá inteligence a datová platforma, jako je například watsonx od IBM, mohou institucím státní a veřejné správy a firmám pomoci využít základní jazykové modely a urychlit tempo zavádění generativní umělé inteligence v celé organizaci. Nedílnou součástí této pomoci je v případě IBM i tým zkušených expertů a odborníků konzultační divize společnosti IBM. Nové funkce a schopnosti watsonx.ai platformy umělé inteligence watsonx od IBM zahrnují nové základní modely pro obecné účely a generování kódu, větší rozmanitost možností modelů s otevřeným zdrojovým kódem a další možnosti dat a možnosti ladění, které mohou rozšířit potenciál a využití generativní umělé inteligence.

Otevřená, důvěryhodná a cílená umělá inteligence

Tato vylepšení byla vedena základními strategickými úvahami IBM, že umělá inteligence by měla být otevřená, důvěryhodná, cílená a posilující. Ředitelé a manažeři pověření zaváděním generativní umělé inteligence potřebují flexibilitu modelu a možnost volby. Potřebují také zabezpečený přístup k obchodním relevantním modelům, které mohou pomoci urychlit čas na získání hodnotných výstupů, jež jim umělá inteligence přinese. V IBM si uvědomujeme, že jednotný přístup nebude vyhovovat všem, a proto poskytujeme našim zákazníkům řadu základních modelů jazyka a kódu různých velikostí a architektur, které klientům pomáhají poskytovat výkon, rychlost a efektivitu.

„V prostředí, kde je prvořadá integrace s našimi systémy a bezproblémové propojení s různým softwarem, se watsonx.ai ukazuje jako přesvědčivé řešení," říká Atsushi Hasegawa, hlavní inženýr vývoje a výzkumu ve společnosti Honda.

Jazykový model Granite od IBM

LLM, tedy velký jazykový model společnosti IBM pro generativní umělou inteligenci, jeho inherentní flexibilita a agilní možnosti nasazení, spolu s robustním závazkem k informační bezpečnosti, zvýrazňují jeho přitažlivost.

Počáteční vydání funkcionality watsonx.ai zahrnovalo rodinu Slate modelů, pouze kodérů užitečných pro podnikové úlohy tzv. NLP, tedy zpracování přirozeného jazyka. Nyní už ale našim zákazníkům nabízíme naši LLM sadu jazykových modelů Granite. Modelová řada Granite je postavena na moderní architektuře a je vhodná pro generativní úkoly jako je sumarizace, generování obsahu, generování rozšířeného vyhledávání, klasifikace a získávání poznatků. Všechny modely Granite byly trénovány na podnikových datových sadách spravovaných IBM. Aby byla zajištěna ještě hlubší odbornost v oblasti, byla rodina modelů Granite vyškolena na podnikových datových sadách z pěti domén: internet, akademické prostředí, kódová, právní a finanční doména, přičemž všechny byly podrobeny kontrole, aby se odstranil nežádoucí obsah, a porovnány s interními a externími modely. Tento proces je navržen tak, aby pomohl zmírnit rizika tak, že výstupy modelu mohou být nasazeny zodpovědně s pomocí watsonx.data a watsonx.governance. Na základě hodnocení a testování IBM Research v rámci 11 různých finančních úkolů výsledky ukazují, že díky školení modelů Granite-13B s vysoce kvalitními finančními daty patří mezi nejvýkonnější modely finančních úkolů a mají potenciál dosáhnout buď podobný, nebo dokonce lepší výkon než mnohem větší modely. Hodnocené finanční úkoly zahrnují například: poskytování skóre sentimentu pro přepisy hovorů o akciích a výdělcích, klasifikaci novinových titulků, extrahování hodnocení úvěrového rizika, shrnutí finančního dlouhého textu a zodpovězení finančních nebo pojišťovacích otázek. K dnešnímu dni mnoho dostupných modelů umělé inteligence postrádá informace o původu dat, testování a bezpečnostních nebo výkonnostních parametrech. Pro mnoho podniků a organizací to může přinést nejistoty, které zpomalují přijetí generativní umělé inteligence, zejména ve vysoce regulovaných odvětvích.

Transparentnost a důvěra

Přístup IBM k vývoji AI se řídí základními principy založenými na závazcích důvěry a transparentnosti. Vzhledem k tomu, že klienti chtějí používat naše modely vyvinuté společností IBM k vytváření diferencovaných aktiv umělé inteligence, doporučujeme klientům, aby dále přizpůsobovali modely IBM tak, aby splňovaly konkrétní následné úkoly. Díky rychlým technikám inženýrství a ladění mohou klienti zodpovědně používat svá vlastní podniková data k dosažení větší přesnosti ve výstupech modelu vytvořit tak pro své organizace a firmy velkou konkurenční výhodu.

Marek Šoule,
marek_soule@cz.ibm.com

STRATEGIE PRO SPRÁVU DAT: PRŮVODCE NA CESTĚ K DOBRÉ PRÁCI S DATY

V minulém čísle jsme představili téma správy dat a popsali, proč je důležité. Tentokrát se zaměříme na obsah dokumentu* Strategie pro správu dat ve veřejné správě České republiky (2024–2030)*, který vláda schválila na konci dubna. Tento dokument dává veškerému úsilí o rozvoj práce s daty ve veřejné správě jasný směr a harmonogram.

MINIMÁLNÍ STANDARD KVALITNÍ SPRÁVY DAT

oblast 0. **ŘÍZENÍ A ORGANIZACE SPRÁVY DAT**

0.1 Je jasně stanovena **odpovědnost za data** úřadu a jejich správu (manažerská, věcná, technická)

0.2 Jsou vydána a v praxi uplatňována základní **interní pravidla** pro správu dat (mj. metadata, kvalita, rizika)

oblast 1. **STANOVENÍ DATOVÝCH POTŘEB**

1.1 Jsou zmapovány a prioritizovány věcné **oblasti dat**

1.2 Jsou stanoveny a řízeny **datové potřeby** v prioritních oblastech

1.3 V rámci informační koncepce úřadu je formulována **strategie v oblasti správy dat**

oblast 2. **POPIS DAT A DATOVÝCH ŘEŠENÍ**

2.1 **Data jsou popsána** a je **definován jejich význam**

2.2 Je vytvořen a využíván **lokální katalog dat** a jeho obsah je součástí národního katalogu dat

2.3 Jsou rozlišeny kategorie dat a procesy správy dat jsou přizpůsobeny jejich specifikům

2.4 V Registru práv a povinností **jsou evidovány agendové údaje** určené ke sdílení

oblast 3. **REALIZACE DATOVÝCH ŘEŠENÍ**

3.1 Úřad **má vytvořeny podmínky pro sdílení požadovaných dat** s jinými úřady

3.2 **Při zadávání a řešení změn** informačních systémů jsou zohledněny dopady na data a jejich správu

oblast 4. **ZAJIŠTĚNÍ A VYUŽITÍ DAT**

4.1 Jsou zavedeny základní postupy pro **zajištění kvality dat**

4.2 Je zavedeno základní **řízení rizik** v oblasti dat

Strategie vznikla s cílem vybudovat solidní základy pro práci s daty v jednotlivých úřadech i na centrální úrovni veřejné správy. Vznikla na základě důkladného poznání aktuálního stavu, dobrých praktik a zkušeností získaných z mnoha stran. Opatřeními navrženými ve strategii chceme rozvinout schopnost organizací veřejné správy dobře o data pečovat a efektivně je využívat. Jde především o schopnost sdílet mezi sebou potřebná data při poskytování služeb veřejnosti. Hned na druhém místě je pak využívání dostupných dat jako podpory pro informovanější rozhodování, ať už k tvorbě politik nebo řízení úřadů.
Dosažení tohoto cíle je běh na dlouhou trať, který jsme začátkem roku 2024 úspěšně odstartovali. Díky vlastní iniciativě i podpoře týmu správy dat Digitální a informační agentury (DIA) už vybrané centrální úřady veřejné správy podnikají kroky, kterými postupně zlepšují znalost, důvěryhodnost a využitelnost svých dat.

Ambice do konce roku 2025

Aktuální úroveň vyspělosti práce s daty v úřadech je velmi rozdílná. Aby mohla veřejná správa v oblasti dat vnitřně fungovat a navenek působit jako jeden kompaktní celek, je nutné v první řadě zajistit, aby všechny úřady spravující nejdůležitější data státu dosáhly alespoň základní úrovně správy dat. Tu označujeme jako *Minimální standard kvalitní správy dat* a skládá se z třinácti bodů shrnujících elementární zásady systematické péče o data.

DIA postupně připravuje k jednotlivým bodům metodické a podpůrné materiály, které vždy doprovází podrobnější výklad ve formě webinářů. Zároveň už od začátku roku 2024 průběžně poskytuje jednotlivým úřadům konzultační i praktickou podporu při uplatňování standardu v jejich podmínkách. Zavádění opatření probíhá postupně a po

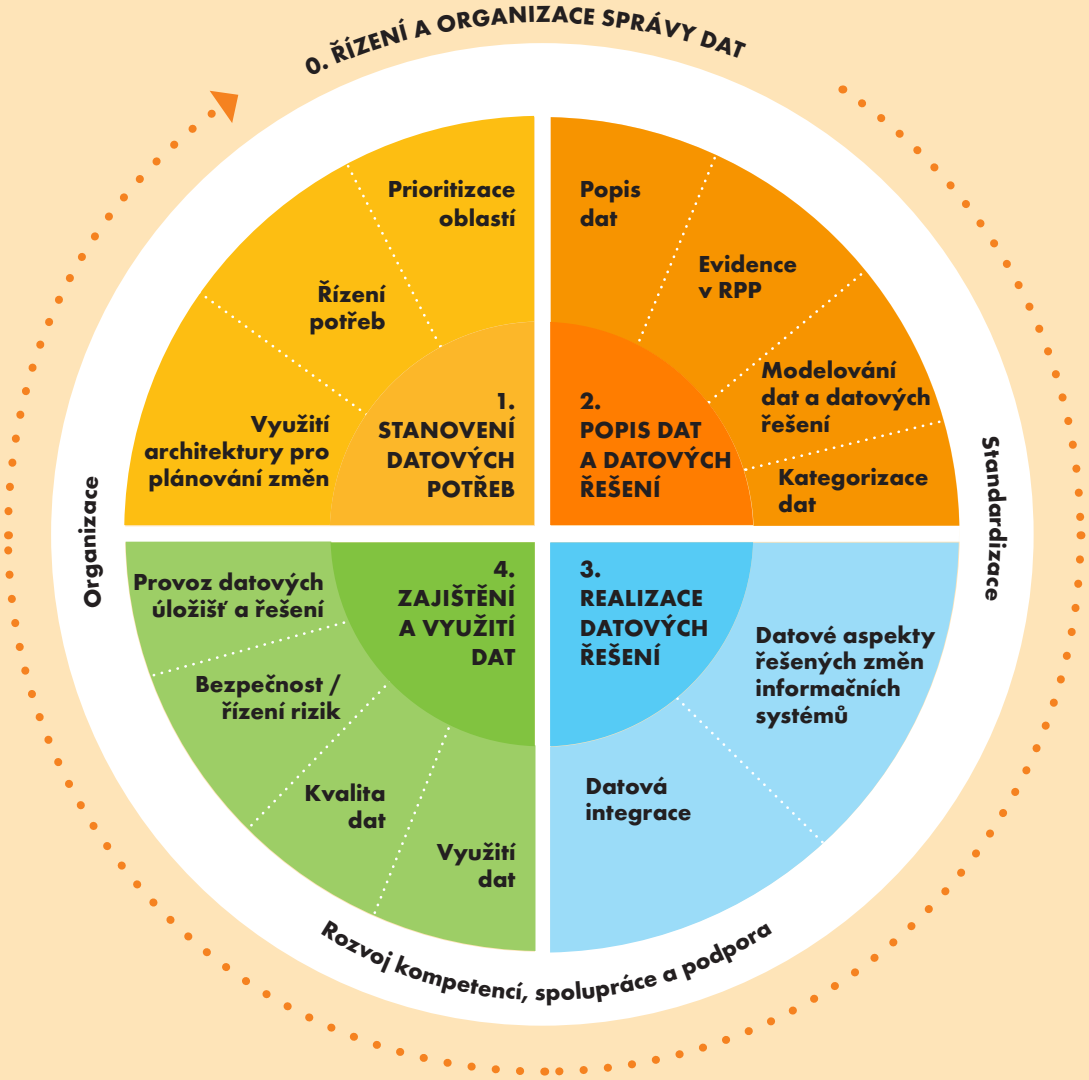
jednotlivých oblastech dat, počínaje těmi, které úřad určil jako prioritní. Cílem společného úsilí je, aby bylo možné v každém z 32 podporovaných úřadů u všech bodů standardu před koncem roku 2025 s klidným svědomím prohlásit: „Ano, toto platí."

Správa dat má široké pole působnosti

Obsah minimálního standardu vznikl „vydestilováním" toho nejnutnějšího z široké škály disciplín a témat, které společně spadají pod označení „správa dat" (angl. „data management"). Pro práci s nimi používáme členění do pěti oblastí, které vychází z mezinárodního metodického rámce DAMA/DMBoK („Data Management Body of Knowledge") a přizpůsobujeme jeho obsah potřebám a specifikům české veřejné správy.

Nezbytným základem systematické práce s daty je „nultá" oblast, **Řízení a organizace správy dat**, ve které se vytváří organizační, procesní a kompetenční předpoklady pro veškerý rozvoj ve zbylých čtyřech oblastech. V oblasti **Stanovení datových potřeb** jde o to správně nasměrovat pozornost a zdroje tam, kde vynaložené úsilí přinese největší užitek (tzn. určit prioritní oblasti a úkoly pro správu dat). Oblast **Popis dat a datových řešení** má za cíl zajistit co nejlepší přehled o datech ve správě úřadu. Ten je nezbytný pro dohledatelnost a správnou interpretaci dat. V oblasti **Realizace datových řešení** je pozornost zaměřena na to, aby byly informační systémy

OBLASTI A TÉMATA SPRÁVY DAT



a integrace mezi nimi řešeny vždy s cílem vytvořit nejlepší možné podmínky pro další práci s daty. Poslední oblast, **Zajištění a využití dat**, pokrývá péči o data při běžném každodenním provozu, ale také vytváření podmínek pro využívání dat a tvorbu analytických produktů.

V každé z těchto oblastí existuje dlouhá řada doporučení, co by měly či mohly organizace dělat pro další zlepšování své správy dat. Strategie ale míří v prvním implementačním období, tj. v letech 2024 a 2025, jen na nezbytné minimum takových doporučení. Jejich výběr i způsob implementace je přizpůsoben potřebám, ale i možnostem a kapacitám vybraných organizací veřejné správy, které se aktuálně zapojily do aktivit na zlepšení správy dat.

I po roce 2025 bude co zlepšovat

V dalším období mezi lety 2026 a 2030 bude třeba kvalitní správu dat postupně rozšiřovat i do zbývajících úřadů, aby také ony splnily alespoň minimální úroveň. Ani pro úřady, které ji splní už na konci roku 2025, však cesta nekončí. V následujícím období budou dále zvyšovat svou úroveň správy a využívání dat. I nadále je v tom bude podporovat DIA, která počítá s rozšiřováním poskytovaných konzultačních služeb, znalostní báze a nástrojové podpory pro správu dat.

Na základě zkušeností s naplňováním strategie v prvním období bude v průběhu roku 2025 připraven detailní implementační plán pro období od roku 2026. Pokročilejší opatření, která by se v něm měla zavádět, jsou však uvedena už v aktuální podobě strategie. Některé úřady totiž dlouhodobě věnují datům velkou pozornost a jsou díky tomu již dnes ve správě svých dat relativně daleko. I těm by měla strategie posloužit jako užitečný ukazatel směru, kterým se má systematická práce s daty ve veřejné správě dále ubírat.

Data jsou ve veřejné správě na vzestupu

Správa a sdílení dat se v červnu letošního roku oficiálně staly jednou z pěti priorit Rady vlády pro informační společnost (RVIS). Zároveň vznikla při RVIS Pracovní skupina pro správu dat. Jejími členy jsou ti zástupci nejvyššího vedení úřadů, kteří jsou celkově manažersky odpovědní za rozvoj správy dat ve svých organizacích. Tato pracovní skupina bude kromě řešení klíčových otázek správy dat a výměny zkušeností také dlouhodobě monitorovat, jak se daří naplňovat cíle strategie. Pevně věříme, že i díky velké pozornosti věnované datům ve veřejné správě se bude jejich správa v nejbližších měsících a letech viditelně zlepšovat, a spolu s ní i schopnost veřejné správy využívat data ve prospěch veřejnosti i vnitřního fungování úřadů.

Podrobnější informace a materiály z oblasti správy dat (včetně samotné strategie) můžete najít na data.gov.cz/správa-dat.

Libor Drlík

Článek vznikl v rámci projektu Zajištění podmínek pro kvalitní správu datového fondu a zajištění řízeného přístupu k datům. Reg. č.: CZ.31.1.01/MV/23_62/0000062 podpořeného Evropskou unií NextGeneration EU.

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 31.12.2024.

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

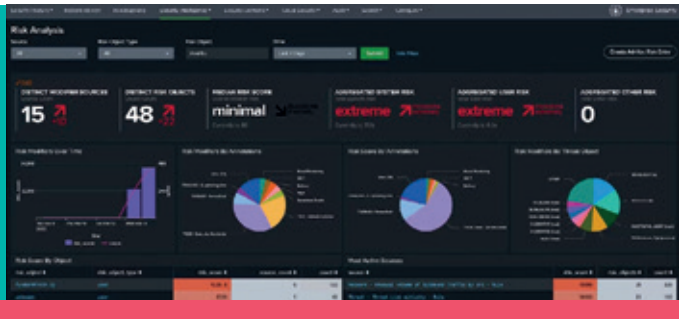
Otestujte si technologii, na kterou sází nejen Ferarri.
Bitdefender chrání více jak 600 Miliónů zařízení po celém světě. Přidejte se k nám.

Trusted. Always.

Rezervujte si konzultaci zdarma

SIEM Essential

Splunk SIEM formou managed služby (SaaS)



Vzhledem ke zvyšující se sofistikovanosti a účinnosti kybernetických útoků, na jejichž odhalení už nestačí používat tradiční nástroje, jakými jsou například IPS (Intrusion Prevention System) nebo antivirus, potřebujete implementovat pokročilejší technologie založené na korelaci velkých dat, umělé inteligenci a strojovém učení.

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

Splunk SIEM byl v tomto roce již podesáté v řadě vyhodnocen jako nejlepší SIEM dle Gartner Magic Quadrant.

PROČ ZVOLIT ŘEŠENÍ SIEM ESSENTIAL OD ALEFu?

Managed služba (Software as a service)

- Dedikovaný tým bezpečnostních specialistů zajišťující provoz a údržbu systému
- Pravidelná aktualizace vyhodnocovacích scénářů dle aktuálních hrozeb
- Efektivní řešení bez vstupních nákladů na implementaci
- Pravidelná aktualizace systému a profylaxe

V případě, že máte zájem o vyzkoušení tohoto produktu formou „proof of value“, kontaktujte nás zde:

SCAN ME

Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8, Česká republika
Phone: +420 225 090 240 | cz-sales@alef.com | www.alef.com
Kontakt: Jan Hrubý | Business Unit Manager | Phone: +420 777 101 037 | jan.hruby@alef.com

*Květen 2023

Hewlett Packard Enterprise

Partner od okraje sítě po cloud

Jedinečně rozmanité portfolio pro výjimečné zážitky

Společnost HPE poskytuje jedinečná, otevřená a inteligentní technologická řešení jako službu. Nabídka zahrnuje cloudové služby, výpočetní techniku, vysoce výkonnou výpočetní techniku a umělou inteligenci, inteligentní koncové body sítě, software a úložiště, s konzistentní uživatelskou zkušeností napříč všemi úložišti a koncovými body, čímž pomáhá zákazníkům rozvíjet nové obchodní modely, zapojovat se novými způsoby a zvyšovat provozní výkon.

Strategický partner pro urychlení digitální transformace

Společnost HPE pomáhá organizacím využívat hodnoty všech dat, ať jsou uložena kdekoli, lépe dosahovat cílů a přizpůsobovat se potřebám zákazníků.

Výpočetní technika: Nabízíme univerzální servery pro různé pracovní zátěže a servery optimalizované pro konkrétní pracovní zátěže, které poskytují nejlepší výkon a hodnotu pro náročné aplikace.

Úložiště: Přetváříme zkušenosti zákazníků s úložišti jako službou a cloudovými datovými službami s nabídkou portfolia, které nabízí primární úložiště, hyperkonvergovanou infrastrukturu, obnovu po havárii a ransomware, řešení pro velké objemy dat, nabídky správy a úložiště pro nestrukturovaná data a analytické úlohy, jakož i tradiční páskové a síťové produkty i disky.

Služby HPE: Poskytujeme poradenství v oblasti digitální transformace, navrhujeme řešení IT a pomáháme podnikům využívat IT jako službu.

HPC&AI: Dodává standardní a zakázková hardwarová i softwarová řešení a řešení pro správu dat určená pro podporu superpočítačů, vysoce výkonných výpočtů (HPC), konvergovaných okrajových systémů a datově náročných úloh, jako jsou aplikace pro analýzu dat a umělou inteligenci.

Inteligentní koncová zařízení: Provozujeme platformy a služby na okrajích sítě, propojujeme zařízení a aplikace prostřednictvím řešení Aruba, jako jsou kabelové a bezdrátové místní sítě, přepínání v areálu a datovém centru, softwarově definované rozsáhlé sítě a zabezpečení sítě.

Cloudové služby HPE GreenLake: Poskytujeme zákazníkům konzistentní cloudové prostředí pro všechny aplikace a data, ať už jsou kdekoli: na okraji sítě, v datovém či kolokačním centru nebo ve veřejných cloudech.

Finanční služby HPE: Jsou finančním motorem nabídek společnosti HPE, který poskytuje finanční řešení včetně nabídek leasingu, správy a recyklace majetku.

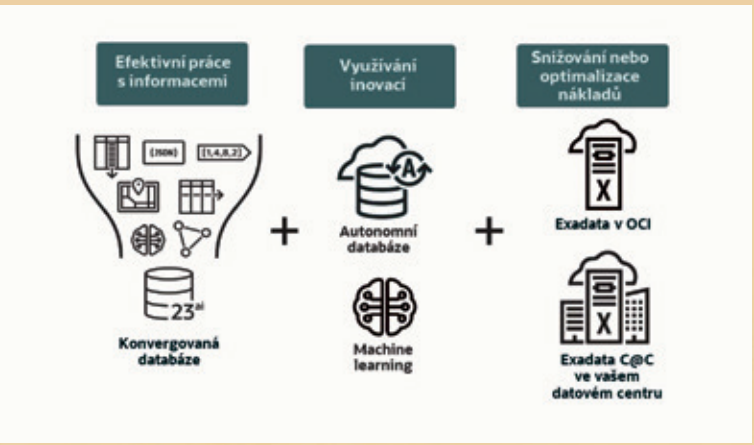
HPE v číslech

28,5 mld. USD čistý výnos ve fin. roce 2022	**>170** států se zákazníky HPE
35 superpočítačů v top 100	Od r. **2022** celé portfolio nabízeno jako služba
99 % společností z Fortune 500 jsou zákazníky	**85 000** prodejních partnerů po celém světě

ORACLE

Platforma Oracle pro veřejnou správu v 21. století

Informační koncepce České republiky z roku 2023 obsahuje několik kapitol, jejichž úspěšné naplnění je podmíněno efektivní prací s informacemi, se kterými státní správa a samospráva pracuje.

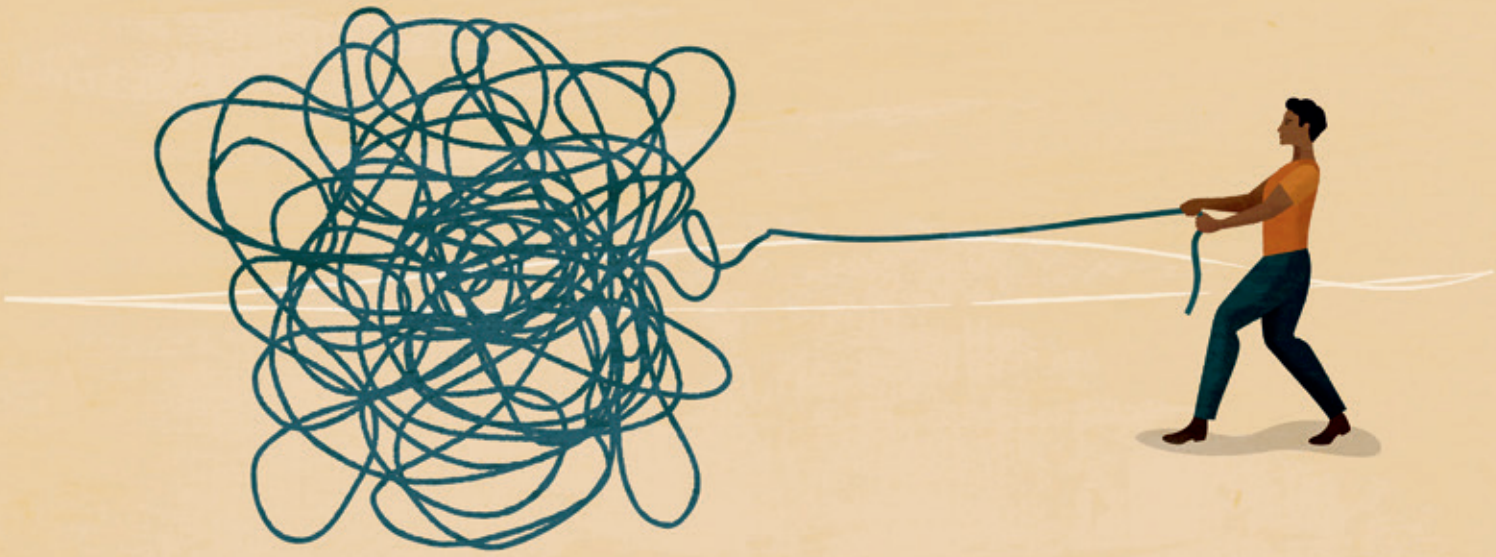


Moderní doba přináší nové výzvy: struktura informací je čím dál tím složitější, výsledky je nutné mít k dispozici v reálném čase a čím dál tím více se prosazují technologie, související s umělou inteligencí a strojovým učením. Do celého tohoto složitého systému vstupuje i ekonomický prvek – náklady na informační technologie se přísně sledují a je neustálá snaha tyto náklady přísně řídit a snižovat.

Společnost Oracle je dlouhodobě světovou jedničkou ve vývoji řešení a produktů, které se zabývají zpracováváním informací. Tato řešení jsou často nasazena pro podporu klíčových aplikací v těch nejkritičtějších oblastech, a to nejen ve státní správě.

Oracle platforma umožňuje práci s libovolným typem dat, libovolným způsobem, kdekoli zákazník potřebuje.

Konsolidace na hybridní platformě Exadata Cloud@Customer je doporučeným strategickým řešením pro informační architekturu, vedoucí k dlouhodobé optimalizaci nákladů na IT.



Informace o Oracle Database 23ai
https://www.oracle.com/database/23ai/

Fortinet Security Fabric je nejvýkonnější platforma kybernetické bezpečnosti v oboru, která poskytuje široké, integrované a automatizované možnosti kybernetické bezpečnosti podporované rozsáhlým otevřeným ekosystémem. Fortinet Security Fabric umožňuje organizacím dosáhnout zabezpečených výsledků v oblasti digitální akcelerace snížením složitosti, zefektivněním provozu a zvýšením schopností detekce hrozeb a reakce na ně.

Více informací na **www.fortinet.com**.

FORTINET


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