DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

servodata
Member of Moore Czech Republic Group

Analýza a porovnání ekonomických a bezpečnostních charakteristik provozu ISVS pomocí cloud computingu, on-premise a klasickým outsourcingem

1. Etapa

Verze 1.4
26.8.2025

Tato verze studie obsahuje pouze vybrané části dokumentu. Detailní analytické kapitoly nejsou zveřejněny z důvodu ochrany důvěrných informací.

Přehled verzí

Verze	Autor	Datum	Verze
1.0	Martina Hábová	25.6.2025	Vydání verze 1.0 (draft)
1.1	Martina Hábová	18.7.2025	Vydání verze 1.1 (draft)
1.2	Martina Hábová	11.8.2025	Vydání verze 1.2 (draft)
1.3	Martina Hábová	18.8.2025	Vydání verze 1.3 (draft)
1.4	Martina Hábová	26.8.2025	Vydání verze 1.4 (final)

OBSAH

1. MANAŽERSKÉ SHRNUTÍ

Dokument je výstupem 1. etapy (pilotní) studie „**Analýza a porovnání ekonomických a bezpečnostních charakteristik provozu ISVS pomocí Cloud Computingu, on-premise a klasickým outsourcingem**“.

Studie měla přispět k potvrzení nebo vyvrácení hypotézy, že provoz ISVS formou cloud computingu je ekonomicky výhodnější a umožňuje snáze dosažení požadované úrovně bezpečnosti ISVS, v detailu tedy:

- Jaké jsou ekonomické a bezpečnostní rozdíly provozování informačních systémů veřejné správy (dále jen „ISVS“) různými formami?
- Je provoz ISVS formou Cloud Computingu výhodnější, než provoz on-premise, a za jakých podmínek?

Studie primárně srovnává cloud computing a on-premise provoz informačních systémů veřejné správy (viz vysvětlení v úvodu kap. 2).

Následující závěry byly formulovány na základě analýzy zkušeností z vybraných zahraničních zemí, diskusemi se zástupci ústředních státních orgánů a analýzou podkladů z vybraných obcí (viz dále v textu této kapitoly).

Jaké jsou ekonomické a bezpečnostní rozdíly provozování informačních systémů veřejné správy různými formami?

Následující charakteristiky jsou předpokladem většiny cloudových strategií implementovaných v analyzovaných zemích (viz kapitola 2.1 Zkušenosti ze zahraničí s implementací cloudu ve veřejné správě).

On-premise řešení vyžadují významné počáteční kapitálové investice zahrnující nákup serverů, síťového vybavení, úložišť, zabezpečovacích nástrojů, a často i výstavbu nebo pronájem specializovaných datových center. Tyto vstupní náklady jsou doplněny rozsáhlými licenčními poplatky za software, které se někdy platí na několik let dopředu. Provozní náklady zahrnují elektřinu, chlazení, internetové připojení, a především personál v podobě IT specialistů a správců systémů, kteří zajišťují nepřetržitý chod infrastruktury. Dodatečné výdaje vznikají při údržbě hardware, nákupu náhradních dílů a pravidelných upgradech, které jsou nezbytné pro udržení výkonu a bezpečnosti systémů, či jako reakce na případné změny.

Hlavní ekonomickou nevýhodou on-premise přístupů je obtížné plánování kapacit, které často vede buď k nákladnému přeinvestování, nebo naopak k nedostatku výpočetního výkonu v kritických momentech. Implementace robustních disaster recovery řešení představuje další významnou finanční zátěž, přičemž organizace často nejsou schopny rychle reagovat na měnící se technologické požadavky bez dalších investic.

Cloud computing naproti tomu nabízí fundamentálně odlišný ekonomický model založený na relativně nízkých vstupních nákladech, které zahrnují i rozpuštěné náklady na zabezpečení na straně poskytovatele, a pay-as-you-use principu (případně obdobnému). Organizace nemusí investovat do vlastního hardware, zabezpečení apod., a místo toho platí měsíční nebo roční předplatné podle skutečného využití služeb. V ceně cloudových služeb jsou obvykle zahrnuty zálohovací služby, automatické aktualizace a technická podpora, což snižuje potřebu vlastních IT specialistů.

Ve sledovaných zemích (viz kapitola 2.1 Zkušenosti ze zahraničí s implementací cloudu ve veřejné správě) bylo cílem koncentrovat datová centra jednotlivých úřadů, zvýšit bezpečnost pro všechny stupně veřejné správy a současně mít přehled o jednotlivých řešeních, které veřejná správa využívá.

Je provoz ISVS formou Cloud Computingu výhodnější, než provoz on-premise, a za jakých podmínek?

Na základě provedené analýzy vyplývá, že provoz ISVS formou Cloud Computingu je ve většině případů výhodnější než provoz on-premise. Obecně platí, že cloudové modely trvale snižují celkové náklady na vlastnictví (TCO), za předpokladu korektního zohlednění všech nákladů hardwaru, softwaru, nástrojů a lidské práce. V praxi to znamená, že při přechodu do cloudu lze ušetřit významné prostředky, protože se eliminují jednotlivé náklady na údržbu a obměnu vlastních datových center a infrastruktury.

Podmínkou výhodnosti je jednak správně smluvně ošetřené cloudové prostředí vhodné pro daný ISVS, které pak nabízí vyšší a konzistentní úroveň bezpečnosti než rozptýlená a často nesjednocená opatření on-premise. Poskytovatelé cloudových služeb pro veřejnou správu musí splňovat přísné standardy a certifikace, což obecně výrazně posiluje bezpečnostní rámec. Současně pak platí, že poskytování standardizovaných balíčků cloudových služeb (SaaS) zvyšuje konkurenci mezi poskytovateli, zvyšuje úspory z rozsahu a zvyšuje efektivitu při provádění změn.

Jak výše úspor, tak zlepšení bezpečnosti jsou silně závislé na způsobu řízení, velikosti organizace a dodržování národních regulačních rámců. Malé úřady často postrádají dostatečné IT experty a provoz vlastního datového centra je pro ně ekonomicky neefektivní (to potvrzují i výsledky z malých českých obcí, viz 2.5.2 Situace v malých obcích), zatímco velké organizace mohou zdůvodnit hybridní přístup nebo specializovaná on-premise řešení. Typ zpracovávaných dat a aplikací rovněž ovlivňuje volbu - kritická infrastruktura může zůstat z bezpečnostních důvodů v on-premise, standardní kancelářské a provozní aplikace jsou vhodné v cloudovém řešení veřejného cloudu. Běžné ISVS jsou někde mezi těmito krajními hranicemi.

Ekonomická i bezpečnostní analýza provozu ISVS ukazuje, že cloud computing při správném nastavení governance, smluvních požadavků a využití ověřených poskytovatelů představuje výraznou cestu k efektivitě i lepšímu zabezpečení. Rozhodující jsou jasné podmínky ve smlouvách, transparentní pravidla migrace a schopnost centrální koordinace i sdílení zkušeností.

Poučení ze zahraničních zkušeností

Zkušenosti z různých evropských zemí ukazují, že migrace na cloudové služby přináší veřejné správě významné úspory nákladů, zvýšení efektivity a zlepšení dostupnosti digitálních služeb. Například ve Švédsku, Dánsku či Estonsku vedla centralizace řízení a sdílení cloudových služeb k efektivnějšímu využívání zdrojů, snížení provozních nákladů a rychlejšímu zavádění nových služeb. Podobně v Německu a Francii umožňuje cloudová strategie snížit provozní a investiční náklady, lépe sdílet infrastrukturu mezi úřady a posílit vyjednávací pozici vůči dodavatelům (viz kapitola 2.1 Zkušenosti ze zahraničí s implementací cloudu ve veřejné správě).

Součástí kapitoly věnující se zahraničí jsou uvedeny rovněž odkazy na externí studie vyčíslující úspory v řádech stovek milionů EUR vyplývající ze snižování provozních nákladů díky konsolidaci datacenter, nižších licenčních poplatků, spotřeby energie apod.

Výhodnost přechodu na cloud je však podmíněna správným nastavením řízení (governance), bezpečnostních standardů a transparentními pravidly pro ochranu dat. Evropské politiky, jako GDPR, NIS 2 nebo Data Act, nastavují vysoké požadavky na bezpečnost a interoperabilitu, což zvyšuje důvěru veřejnosti a ochranu citlivých údajů. Zároveň zkušenosti ukazují, že úspěšná cloudová transformace vyžaduje systematickou podporu migrace IS a dat, vzdělávání zaměstnanců a centralizované řízení změn. V případě některých systémů, resp. dat, se však může ukázat, že cloud není vhodným řešením nebo je nutné posoudit jaký typ cloudu zvolit (stupeň bezpečnosti).

Celkově lze však uzavřít, že přechod veřejné správy na cloud v evropském kontextu je ekonomicky i provozně výhodný, pokud je realizován v souladu s moderními bezpečnostními a správními standardy a s ohledem na odstupňované požadavky na digitální suverenitu a bezpečnost.

Závěr z využití kalkulace TCO

Zpracování TCO je v ČR povinným parametrem hodnocení provozu ISVS, v zahraničí může být využití TCO mírně odlišné.

Zpracovatelé tradičních analýz celkových nákladů vlastnictví se přitom zaměřují především na přímé kapitálové a provozní výdaje, ale mohou opomíjet klíčové nákladové položky, které mohou představovat značnou část celkových investic; např. migrační náklady mohou zahrnovat nutné úpravy aplikace původních systémů pro cloudový provoz či paralelní provoz starého i nového prostředí po dlouhou dobu. Compliance požadavky generují náklady na legislativní audity, certifikace a jejich pravidelné obnovování každé 2-3 roky. Rizikové faktory jako vendor lock-in mohou stát 10-20% původního rozpočtu, zatímco kybernetické incidenty představují riziko v obrovských částkách.

Současně zpracovatelé konvenčního TCO často nedokáží ocenit strategické přínosy jako business agility, zkrácení time-to-market, zlepšenou uživatelskou spokojenost nebo environmentální dopady - snížení energetické stopy.

Neúplné TCO analýzy vedou ke konzervativnímu rozhodnutí setrvat u tradičních řešení, přeceňování výhod on-premise apod. Podrobněji kapitola 2.3 Celkové náklady vlastnictví (TCO).

Nedostatečně zpracovaná TCO analýza, která vychází z nesprávných nebo neúplných dat, může vést k závažným dlouhodobým negativním důsledkům:

- Rozpočtové problémy - nepředvídané náklady ve výši desítek procent nad původní rozpočet, nutnost dalších investičních výdajů nebo rozpočtových škrtů. Prodloužení harmonogramů - skluz projektů o měsíce až roky, zpomalení zavádění nových služeb. Ztráta důvěry veřejnosti - opakované překročení rozpočtu oslabuje důvěru v digitalizaci státu.
- Bezpečnostní rizika - šetření na bezpečnostních opatřeních zvyšuje pravděpodobnost výpadků a úniků dat. Vendor lock-in - finanční a technická závislost na jednom dodavateli omezuje flexibilitu. Nadměrné provozní náklady - dlouhodobé provozování zastaralých technologií.

Většina veřejných institucí není schopna připravit komplexní TCO kvůli omezeným interním kapacitám, kdy nedostatek specializovaných expertů způsobuje neschopnost zmapovat všechny nákladové položky, rozložení odpovědnosti za jednotlivé náklady mezi různá oddělení bez centrální koordinace či skryté položky jako jsou pravidelné audity či testování bezpečnosti.

Když nelze spolehlivě sestavit TCO, je vhodné jej doplnit na **vícekriteriální rozhodovací rámec**, který zohledňuje nejen finance, ale i strategické, provozní, bezpečnostní a organizační aspekty. Tento přístup překonává limity TCO zaměřením na širší přínosy a rizika, umožňuje flexibilní aplikaci podle velikosti úřadu a typu agendy a podporuje vyvážené rozhodování prostřednictvím bodového hodnocení jednotlivých faktorů. Více podrobností k vícekriteriálnímu rozhodování viz kap. 2.3.5.

Závěry ze srovnání úrovně zabezpečení

Z bezpečnostního hlediska nabízí on-premise řešení organizacím přímou kontrolu nad celou infrastrukturou včetně fyzického přístupu k serverům a možnosti implementace vlastních bezpečnostních politik. Při uplatnění nejpřísnějších politik lze zajistit, aby data organizace byla ukládána i zpracovávána pouze v jejím fyzickém perimetru, avšak v praxi je tento požadavek dnes již obtížné zajistit. Vedoucí pracovníci často vyžadují dálkový přístup odkudkoli (z notebooku nebo z chytrého telefonu) a čím dál častěji se i u těchto organizací začínají využívat externě poskytované služby nebo nadrezortní týmová spolupráce. Vzhledem k častým přenosům (zpracování) dat mimo organizaci je tak i zde stále těžší prosazovat bezpečnostní politiku „opevněného hradu s vodním příkopem“ a zcela tak eliminovat rizika zneužití interních dat. Jako kompromis může být zavedena politika ukládání (a výjimečně i veškeré zpracování) citlivých dat organizace pouze v interních úložištích (on-premise), což pak usnadňuje splnění specifických compliance požadavků a zvyšuje kontrolu nad síťovým provozem.

Tento přístup může být preferován u kritických systémů nebo v případech, kdy regulatorní požadavky vyžadují lokalizaci dat na národním či EU území.

Nevýhodou on-premise zabezpečení jsou však omezené zdroje, které ztěžují implementaci pokročilých bezpečnostních řešení a udržování specializovaného personálu. Mnoho organizací trpí nedostatkem kybernetických expertů a nedokáže rychle reagovat na nové hrozby. Rizika zahrnují single point of failure, lidské chyby při konfiguraci systémů a postupné zastarávání bezpečnostních postupů.

Cloud computing poskytuje přístup k profesionálnímu zabezpečení prostřednictvím specializovaných bezpečnostních týmů, které pracují nepřetržitě a mají k dispozici pokročilé monitorovací systémy. Poskytovatelé cloudových služeb investují značné prostředky do automatických bezpečnostních systémů, sdílení informací o nejnovějších hrozbách či rychlého nasazování bezpečnostních záplat. Většina renomovaných poskytovatelů má nejrůznější certifikace podle mezinárodních standardů (viz dále kapitola 2.4. Bezpečnostní aspekty).

Pro potřeby evropských organizací lze cloudové prostředí rozdělit do čtyř stupňů naplnění požadavků na „datovou suverenitu EU“ podle míry kontroly nad zpracováním a ukládáním dat, geografického omezení provozu, a dle požadavků na podpůrný personál. Vzhledem k těmto omezením by si zákazníci v EU vždy měli ověřit míru ochrany proti přístupu non-EU orgánů, dostupnost platformních služeb v dané implementaci „suverénního“ cloudu či cenovou politiku včetně možných příplatků.

Pouze na základě těchto informací (právní podmínky, rozsah služeb, cenový příplatek) lze kvalifikovaně rozhodnout, zda je konkrétní cloudová nabídka vhodná pro daný informační systém požadované úrovně zabezpečení (viz kapitola 2.2.1 Strategie non-EU poskytovatelů cloudových služeb).

Závěry významné pro centrální úřady a velká OVS

Ústřední orgány státní správy pro účely studie neposkytly žádné nákladové rozpočty potřebné pro objektivní srovnání původních on-premise prostředí s cloudovými řešeními. Tato absence dat představuje zásadní překážku pro přímé ekonomické hodnocení (viz kapitola 2.5.1 Situace u ústředních orgánů státní správy).

Zástupci těchto úřadů argumentují, že původní systémy nejsou srovnatelné s novými díky upgradům funkcionalit a změnám vnitřní architektury.

Další problém spočívá v neschopnosti sestavit TCO kalkulačku z důvodu roztříštěnosti informací o nákladech napříč různými částmi úřadu. Systémové problémy TCO kalkulací dle provedených rozhovorů se zástupci ústředních orgánů či jejich dodavatelů zahrnují:

- neúplné zachycení bezpečnostních nákladů,
- provozní efektivita jednotlivých ISVS vs. celkové náklady na provoz IS úřadu,
- rozdílná vnímání rizik při aplikaci přiměřeného zabezpečení.

Souvisejícím argumentem jsou strukturální překážky přechodu na cloud:

- financování CAPEX-OPEX,
- vendor lock-in a monolitické agendové systémy,
- manažerské faktory,
- obavy ze splnění požadavků v oblasti Compliance.

V případě zkoumání u ústředních orgánů veřejné správy ČR tedy nelze kvůli nedostatku informací jednoznačně potvrdit ekonomickou výhodnost přechodu na cloudový provoz. Při rozhodování o přechodu na cloud nebo setrvání v on-premise prostředí bude nutné zvážit i další aspekty s ohledem zejména na kritičnost systému a naplnění strategických cílů (viz vícekriteriální rozhodování, kapitola

2.3.5 Shrnutí). Absence podmínek pro sestavení podrobných a úplných TCO kalkulací na straně zástupců veřejné správy odráží náročnost a komplexnost samotného problému.

Závěry významné pro malé OVS (obce 1. a 2. typu)

Analyzované **obce do 2 000 obyvatel** (viz kapitola 2.5.2.1 Obce do 2 000 obyvatel) vykazovaly společné charakteristiky. Ve výchozí situaci provozovaly "ploché sítě" s několika počítači a tiskárnami, zastaralé systémy s nižší úrovní zabezpečení. Nedostatečná segmentace sítě a absence moderních bezpečnostních nástrojů zvyšovala riziko vniknutí malwaru či ransomwaru.

Ekonomické vyhodnocení – kvůli nízké kvalitě podkladů a přítomného zabezpečení bylo nutno zpracovat odhad nutného hardware on-premise v souladu se zadáním studie. Byl uvažován vlastní server s potřebnými licencemi, zálohováním a náklady na housing, a to v MIN a MAX variantě.

Ve všech pěti zkoumaných obcích vychází cloudové řešení jako výhodnější varianta provozu v porovnání s dostatečně zabezpečeným on-premise systémem. Zdánlivě výhodný zastaralý on-premise provoz se z hlediska bezpečnosti ukazuje jako dlouhodobě neudržitelný. Při započítání odhadu nutných nákladů na zavedení dodatečných bezpečnostních opatření vychází provoz v on-premise prostředí jako jednoznačně dražší. Úspory se v těchto zkoumaných obcích pohybovaly nejčastěji ve výši 35 – 55 %.

Situace ve zkoumaných **obcích do 5 000 obyvatel** (viz kapitola 2.5.2.2 Obce do 5 000 obyvatel) byla výrazně odlišná. Tyto obce měly ve výchozí situaci značně zainvestováno do serverů, potřebných licencí souvisejících s provozem ISVS a vyřešený housing (bezpečnost datových center). IT prostředí se dalo označit za vyhovující i z hlediska bezpečnosti.

Ekonomické vyhodnocení – díky dostupným podkladům zpracovatel mohl přímo využít údaje poskytnuté obcemi pro srovnání skutečných nákladů vynaložených na on-premise provoz s náklady na cloud computing. Z pohledu bezpečnosti považují zástupci obou obcí situaci za srovnatelnou, přičemž převládá výhoda na straně cloudu z důvodu stálého monitoringu prostředí. K dalším výhodám může patřit zajištění služeb 24x7 či bezpečné přihlašování do systému z míst mimo úřad. V případě obou obcí vychází cloudové řešení jako výhodnější varianta provozu. Úspory se v těchto zkoumaných obcích pohybovaly ve výši 50 – 80 %.

Na základě výše uvedeného lze doporučit systematický přechod na cloud computing s prioritou pro malé obce, které z něj budou mít největší přínos, a postupnou migraci ústředních orgánů s ohledem na specifika jejich agendových systémů.

2. PŘEHLED ZJIŠTĚNÍ A ZÁVĚRŮ

Následující kapitola shrnuje klíčová zjištění studie „**Analýza a porovnání ekonomických a bezpečnostních charakteristik provozu ISVS pomocí cloud computingu, on-premise a klasickým outsourcingem**“.

Studie původně dle názvu zahrnovala i model klasického outsourcingu, avšak v úvodní fázi výzkumu bylo po dohodě se Zadavatelem **rozhodnuto tuto variantu ze závěrečných výstupů vypustit**. Důvodem je, že v praxi digitální transformace a modernizace IT systémů ve veřejné správě i v komerčním sektoru je hranice mezi tradičním outsourcingem IT služeb a cloud computingem stále méně zřetelná. Důvodem je nejen technologický pokrok, ale i povaha aktuálních projektů, které často využívají hybridní přístup nebo přecházejí do cloudu postupně.

Cloud je sám formou outsourcingu - historicky bylo outsourcingem míněno svěřování vývoje, provozu nebo správy určité části IT infrastruktury nebo aplikace externímu dodavateli mimo organizaci. S nástupem modelů SaaS, PaaS, IaaS aj. se logicky cloud computing stává pouze jeho mladší, technicky vyspělejší variantou – organizace nedrží infrastrukturu ani software u sebe a využívají externě poskytovanou službu, která může být cenově efektivnější díky úsporám z rozsahu.

Mnoho úřadů veřejné správy a řada větších firem už dávno outsourcuje a často jen přesune systém z datového centra externího partnera do veřejného cloudu podle ZoISVS, popř. se i původní externí partner stane poskytovatelem cloud computingu podle ZoISVS. Přechod může mít také několik fází.

Přípravná-fáze: lift & shift - prvním krokem může být jednoduché přesunutí „legacy“ systému do cloudového prostředí bez změny jeho architektury (tzv. „lift & shift“), typicky v situacích, kdy končí životnost hardware či hostingová smlouva, dochází místo v datacentru, roste tlak na bezpečnost nebo flexibilitu služeb, a to v případě, že to stávající technologie a architektura systému dovoluje.

V prvním kroku přechodu na cloud computing se pro uživatele ani správce systému zdánlivě mnoho nemění – fakticky je to outsourcing nicméně s tím rozdílem, že infrastruktura je nyní plně virtualizovaná, sdílená pro různé organizace (zákazníky), a přímo nastavitelná správci jednotlivých organizací. Rozdíly, zejména z hlediska zajištění bezpečnosti na sdílené infrastruktuře, musí být uvedeny ve smlouvě. Kromě toho, jakmile je naplněna definice cloud computingu podle ZoISVS (tedy alespoň na vrstvě IaaS), mají OVS povinnost využívat ve většině scénářů pouze zapsané služby od prověřených a zapsaných poskytovatelů cloud computingu.

Teprve ve druhé fázi – refaktoring a modernizace - teprve následně je často zahájen proces skutečné modernizace aplikace (refaktoring): systémy jsou rozbíjeny do menších služeb, upgradovány na cloud-native architekturu (mikroslužby, API-first přístup, serverless, kontinuita DevOps automatizace apod.). V této chvíli se začínají užívat všechny výhody cloudu – lepší škálování podle zátěže, automatizované zálohy, dynamická bezpečnost, vysoká dostupnost a zejména pružnější integrace s dalšími systémy. Až zde lze mluvit o „plnohodnotném cloud computingu“ v protikladu k původní fázi přenosu aplikace na infrastrukturu externího poskytovatele.

Mnoho projektů (zvlášť ve veřejné správě) je ve svém přechodu do cloudu limitováno požadavky na uchování dat, audit, zajištění kontinuity služeb a přechodné období, kdy části systému zůstávají provozovány původním způsobem, jiné už v cloudu. Zkušenosti z evropských projektů zmiňují, že cloudový model se často nastavuje ve více etapách – v první fázi je hlavní cíl rychle splnit compliance a snížit náklady, teprve ve druhé a třetí fázi je možné řešit optimalizaci aplikací, využití automatizace CI/CD, AI a dalších cloud benefitů.

V důsledku tohoto překryvu často dochází k nedorozuměním – např. v zadávací dokumentaci není jasně určeno, jaké části systému se mají refaktorovat, co stačí „jen přesunout“ a jaké bezpečnostní/organizační dopady lze očekávat.

2.1 Zkušenosti ze zahraničí s implementací cloudu ve veřejné správě

V rámci hodnocení zahraničních zkušeností s implementací cloudu byly vybrané evropské země pracovně rozděleny do skupin, které se vyznačují obdobným přístupem, politikami a metodikami. Toto rozdělení zahrnuje severní model zastoupený Švédskem, Dánskem a Estonskem, konzervativní hybrid reprezentovaný Německem a Francií, a transformační model charakterizovaný Itálií. Dále byla doplněna Velká Británie s pozicí aktuálně mimo EU.

V posledním desetiletí prošla evropská veřejná správa rozsáhlou digitální transformací, v jejímž jádru stojí přechod na cloudové technologie. Různé země zvolily odlišné modely: Spojené království prosazuje mandatorní „Cloud First“ přístup s centralizovanou autoritou GDS (Government Digital Service) a digitálním tržištěm G-Cloud, Německo uplatňuje federovaný[1] hybridní cloud, který je provozován především centrálním celostátním IT místem ITZBund, dále státními podniky jako např. Dataport, a také zahrnuje soukromé poskytovatele certifikovaných služeb pod národním standardem BSI C5. Francie opustila záměr jednoho státního poskytovatele a certifikuje soukromé poskytovatele podle přísného standardu SecNumCloud a implementuje cloudová řešení (projekty jako S3NS, Bleu[2] a další), kde Gaia-X slouží jako standard a nástroj pro výměnu dat. Itálie realizuje centralizovaný transformační model s cílem migrovat 75% veřejných správ do Polo Strategico Nazionale a kvalifikovaných komerčních cloudů, zatímco Dánsko, Švédsko, Estonsko preferují realizaci státního cloudu prostřednictvím konsorcií ovládaných národními agenturami, a to paralelně s rámcovými smlouvami s komerčními poskytovateli. Kromě toho Dánsko rozvinulo nový model společného financování cloudových služeb, provozovaných konsorciem KOMBIT jakožto účelové neziskové organizace pod dánským svazem měst a obcí.

Analýza těchto přístupů ukazuje nejen finanční výhody cloudu – výrazné úspory nákladů a efektivnější využití prostředků, ale i provozní přínosy, jako je vyšší škálovatelnost, rychlejší nasazení nových služeb a lepší dostupnost digitálních řešení pro občany. Klíčovou otázkou však zůstává bezpečnost: evropské politiky (GDPR, NIS 2, Data Act) nastavují přísné požadavky na ochranu dat, kybernetickou odolnost i interoperabilitu, což je v jednotlivých modelech zajišťováno skrze národní certifikace, end-to-end šifrování, řízení přístupů a povinné audity.

Zkušenosti ze Švédska, Dánska a Estonska ukazují, že centralizace a financování dle počtu obyvatel obce podporují rovnoměrný přístup k technologiím a snadné sdílení znalostí - kombinují vysokou digitalizaci s propracovanými bezpečnostními opatřeními, přičemž prioritizují funkčnost a efektivitu při zachování bezpečnostních standardů. Konzervativní hybridní přístupy v Německu a Francii jsou „strategicky opatrné“ - kladou důraz na suverenitu a compliance jako základní předpoklady digitální transformace. Italský transformační model demonstruje sílu masové migrace řízené jednotnou metodikou EMG2C, podporovanou robustní finanční injekcí z PNRR. Srovnání těchto strategií poskytuje cenné poznatky o tom, jak kombinace správného finančního modelu, governance, standardizace a bezpečnostních opatření vede k úspěšné cloudové transformaci veřejné správy.

2.1.1 Severní model: Švédsko, Dánsko, Estonsko

(více detailů obsahuje kapitola 3.1 Severní model)

Centralizace a sdílené služby jako základ strategie

Severní model se vyznačuje silnou centralizací řízení a založením národních agentur či konsorcií, která centrálně provozují a spravují sdílené cloudové služby pro ústřední orgány i pro regionální a místní samosprávy. Tato strategie zajišťuje jednotnost přístupu a efektivní využívání zdrojů napříč všemi

[1] https://xpert.digital/en/multi-cloud-strategy/

[2] https://newsroom.orange.com/capgemini-and-orange-announce-plan-to-create-bleu-a-company-to-provide-a-cloud-de-confiance-in-france/

úrovněmi veřejné správy. Kromě toho tyto agentury či konsorcia zajišťují rámcové smlouvy s kvalifikovanými komerčními poskytovateli (vč. U.S. hyperscalerů).

Švédsko:

DIGG (Myndigheten för digital förvaltning) je vládou pověřena vydáváním právně závazných metodik, technických rámců a rámcových smluv pro veřejný sektor ve Švédsku a dohlíží na plnění národních digitálních strategií, včetně obecného sledování migrace digitálních služeb do cloudu. DIGG může hrát roli facilitátora inovací, crowdsourcingu znalostí a testování nových digitálních řešení za účasti veřejného i soukromého sektoru[3].

DIGG vydává rámcové pokyny a standardy pro veřejný sektor, který si jednotlivé cloudové služby (IaaS, PaaS, SaaS) vybírá sám v rámci veřejných zakázek nebo rámcových smluv.

Základní principy financování - klíčové investice do digitální infrastruktury (síťová propojení, datová centra, cloudové služby) jsou financovány přímo ze státního rozpočtu a z účelových fondů na rozvoj digitálních technologií. Stát i samosprávy (kraje a obce) společně investují do cloudových služeb potřebných pro veřejnou správu a často vytvářejí sdružené projekty (například pro oblast zdravotnictví či školství), kde se náklady sdílí mezi zapojené organizace.

Dánsko:

Koordinátorem digitalizace včetně cloudových služeb je v Dánsku Agentura pro digitalizaci (Digitaliseringsstyrelsen), která spadá pod Ministerstvo financí[4]. Agentura metodicky vede, koordinuje a dozoruje digitalizaci, správu ICT projektů a nasazování cloudových řešení pro celou veřejnou správu; vydává závazné strategie a technické rámce.

GovCloud Denmark představuje centrálně provozovaný „community cloud“, spravovaný státní agenturou Statens IT, jež je vyžadována či preferována zejména pro centrální ministerstva a agentury. Veřejné instituce v Dánsku mohou využívat také komerční cloudové služby, pokud tyto splňují jistá bezpečnostní opatření. Agentura pro digitalizaci (Digitaliseringsstyrelsen) vydala konkrétní průvodce a metodiky, jak bezpečně vybírat, hodnotit a provozovat i tyto veřejné (public) cloudy v souladu s právními a bezpečnostními požadavky státu[5].

Další klíčovou organizací v Dánsku je účelová nezisková organizace KOMBIT[6]. Jedná se o plně funkční sdruženou organizaci vlastněnou všemi dánskými municipalitami přes KL (Kommunernes Landsforening). KOMBIT vytvořil protiváhu a konkurenci proti de facto monopolnímu dodavateli pro veřejnou správu KMD A/S. Posláním KOMBIT je sjednocovat poptávky, realizovat centrální výběrová řízení, a hlavně vyvíjet a provozovat společné IT systémy pro všechny obce najednou. Obdobná úroveň vlastního zajišťování IT řešení v takovém rozsahu a napříč celou komunální sférou je v evropském kontextu jedinečná. KOMBIT vyvíjí a provozuje více než 30 informačních systémů pro města a obce a také pro vzdělávání[7] − například platformu pro školy (Aula), agendy pracovních neschopností a sociálních dávek, knihovny či sdílené registry. Správa i další rozvoj jsou řízeny sdružením obcí KL – Kommunernes Landsforening se zapojením všech „city councils“, což je oproti evropským zemím s roztříštěnou strukturou zvláštní výhoda. KOMBIT přitom nepotřeboval masívně investovat do vlastních

[3] https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/05/digital-government-review-of-sweden_7917ba3f/4daf932b-en.pdf

[4] https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Denmark_vFinal_0.pdf

[5] https://en.digst.dk/digital-governance/new-technologies/guide-on-the-use-of-cloud-services/

[6] https://leadiq.com/c/kombit-as/5a1d8933240000240062b0b7

[7] https://systematic.com/int/industries/library-learning/news-knowledge/news/systematic-re-wins-valuable-contract-for-denmark-s-library-system/

datových center – využívá podle citlivosti agend primárně infrastrukturu státního poskytovatele Statens IT nebo infrastrukturu kvalifikovaných soukromých poskytovatelů.

Základní principy financování - na každém IS projektu se před jeho zahájením dohodnou jednotlivé obce, které garantují svou účast a budoucí využití systému. Projekt je zahájen pouze tehdy, když se pro něj přihlásí dostatečný počet obcí, čímž je zajištěna ekonomická efektivita a sdílení nákladů napříč samosprávou[8]. KOMBIT sám nese riziko a náklad spojený s vývojem a implementací IT řešení. Obce začínají platit až ve chvíli, kdy je systém úspěšně nasazen a používán. Díky tomu samosprávy nenesou riziko neúspěšné investice, což vytváří ochranný mechanismus pro veřejné finance. Náklady za provoz, rozvoj a údržbu systémů dodávaných KOMBITem jsou obcím fakturovány na základě jasných smluv a rozpočtů. Výhodou je kumulativní efekt, tedy čím více obcí službu využívá, tím výhodnější jsou podmínky díky sdílení nákladů mezi všemi klienty[9].

Estonsko:

Hlavní role v řízení cloudové infrastruktury a digitálních služeb má Estonian Government IT Centre (RIT) a Státní nadace pro infokomunikace (RIKS). Tyto instituce zajišťují centrální správu vládního cloudu (Estonian Government Cloud - Riigipilv[10]), rámců bezpečnosti a katalogizaci cloudových služeb. RIKS a RIT spravují infrastrukturu, provozní bezpečnost (dle standardu ISKE) a koordinaci napříč všemi úrovněmi státní správy – od ministerstev až po jednotlivé obce a města[11]. Úřady využívají pro strategická a citlivá data primárně státní cloud Riigipilv, ale pro méně citlivá smí využívat rovněž komerční cloudy jako MS Azure, AWS, Google. Odpovědnost za výběr vhodné platformy je na jednotlivých úřadech a jejich posouzení rizik.

Státní cloud Riigipilv byl vybudován v partnerství státu a předních soukromých firem, které společně s RIKS tvoří konsorcium (Cybernetica, Dell EMC, Ericsson, OpenNode, Telia). Kromě toho RIT nabízí i centralizovanou podporu pro vstupní body k veřejným cloudům jako jsou Microsoft Azure a AWS, a zajišťuje k tomu i základní bezpečnostní opatření[12].

X-Road[13] je klíčovou softwarovou platformou pro bezpečnou a interoperabilní výměnu dat mezi všemi informačními systémy estonského státu, včetně systémů v Estonian Government Cloud. Funguje nezávisle na tom, zda systémy běží v cloudu nebo on-premise.

Základní principy financování – estonské úřady hradí náklady za cloudové služby prostřednictvím kombinovaného modelu, který spojuje centrální financování strategické infrastruktury se sdílením provozních nákladů podle skutečného využití.

Základní investice do Government Cloud (Riigipilv) jsou hrazeny ze státního rozpočtu s podporou EU fondů a veřejně-soukromých partnerství, zatímco úřady platí pouze za skutečně využité služby na bázi pay-as-you-go modelu. Estonian IT Centre (RIT) koordinuje tento systém prostřednictvím centralizovaných rámcových zakázek a pokrývají všechny státní IT organizace. Tyto společné nákupy jsou výrazně nákladově efektivnější než separátní zakázky jednotlivých úřadů.

Úřady konkrétně hradí provozní náklady za využívané cloudové služby, podíl na údržbě a rozvoji systémů a náklady na bezpečnostní opatření a monitoring. Flexibilní přístup typu pay-as-you-use

[8] https://www.bus-ex.com/article/kombit

[9] https://offentligsektorsdataforum.wordpress.com/wp-content/uploads/2015/12/9-3-kommunernes-it-fc3a6llesskab-kombit.pdf

[10] https://www.riigipilv.ee

[11] https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Estonia_vFinal.pdf

[12] www.rit.ee/en/news/estonian-public-sector-opens-door-public-cloud-services

[13] https://e-estonia.com/solutions/e-governance/government-cloud/

znamená, že instituce nemusí investovat do vlastní IT infrastruktury a mohou rychle škálovat podle potřeb bez velkých kapitálových výdajů.

Komplexní podpora migrace a systematické vzdělávání

Každá země v rámci severního modelu zřídila centrální týmy a programy zaměřené na metodickou podporu migrace, poskytování šablon smluv a realizaci masivních vzdělávacích iniciativ. Tato systematická podpora je nezbytná pro úspěšnou transformaci veřejné správy.

Švédsko prostřednictvím DIGG provozuje e-Gov Academy, která nabízí online kurzy v oblasti cloudových bezpečnostních úrovní, vzorové smlouvy a roadmapy migrace legacy systémů. Tento přístup zajišťuje, že všichni účastníci mají přístup ke kvalitním vzdělávacím materiálům a metodické podpoře.

Dánsko kombinuje síly KOMBIT a Digitaliseringsstyrelsen v nabídce konzultací, workshopů a certifikovaného výcviku "DigitaliseringsPartnership" pro IT manažery a úředníky. Součástí jsou i testovací sandboxy v rámci Shared Cloud, které umožňují praktické ověření řešení před jejich nasazením.

Estonsko koordinuje prostřednictvím RIA tzv. "e-School" programy pro úředníky, provozuje X-Road akademii a vydává podrobné migrační manuály založené na metodice EMG2C (Explore, Make, Go-to-Cloud) pro všechny veřejné administrativy.

Digitální suverenita jako strategická priorita

Ochrana dat a jejich lokalizace jsou klíčovými součástmi národních strategií severního modelu. Tyto země usilují o kontrolu nad přístupy k datům a snížení závislosti na neevropských providerech, aniž by přitom vyloučily využívání služeb globálních poskytovatelů.

Poznámka 1: Důraz na digitální suverenitu neznamená, že jsou vyloučeni poskytovatelé jako Microsoft, AWS apod., ale že musí splnit určitá pravidla, přičemž některá řešení již existují. viz kapitola 2.2.1 .

Poznámka 2: Estonská podpora distribuovaného řešení (včetně geografického řešení) vyústila až do vzniku estonského datového velvyslanectví v Lucembursku. viz kapitola 2.2.2.

Úspory nákladů v severním modelu

Švédsko – Analýza firmy Radar z roku 2021[14], která hodnotí efektivitu digitalizace a využívání cloudových služeb ve veřejné správě uvádí, že v letech 2018–2020 docházelo ke ztrátám efektivity ve výši přibližně 4,6 miliardy SEK (cca 440 milionů EUR) kvůli nízkému využívání cloudových technologií a neefektivnímu provozu vlastních datových center. Dále uvádí, že každých šest měsíců právní nejistoty stojí sektor asi 1,1 miliardy SEK (cca 105 milionů EUR).

Dánsko – Studie Copenhagen Economics z roku 2022[15], která analyzuje ekonomické přínosy digitalizace a cloudových služeb. Podle ní dosahuje dánský veřejný sektor úspor 30–40 % v celkových nákladech na vlastnictví IT oproti provozu vlastních serverů a datových center. Roční úspory pro různé velikosti organizací jsou odhadovány na 110 000 DKK (cca 15 000 EUR) pro mikrofirmy a 2,6 milionu DKK (cca 350 000 EUR) pro velké instituce. Celkový odhadovaný ekonomický přínos cloudových služeb je přibližně 6,5 miliardy DKK ročně (cca 870 milionů EUR).

Estonsko – Příklady a analýzy z evropských benchmarků a vládních zpráv, které uvádějí, že Estonsko je považováno za lídra v digitalizaci veřejné správy. Přechod na centrální vládní cloud umožnil výrazné snížení provozních nákladů díky centralizaci, škálovatelnosti a efektivní správě IT infrastruktury. Přesná

[14] Radar, "Digital Government Efficiency Report", 2021 (dostupné na https://radar.se/digital-government-efficiency)

[15] Copenhagen Economics, "Public Sector Cloud Savings", 2022 (https://copenhageneconomics.com/public-sector-cloud-savings)

čísla o úsporách nejsou ve veřejných zdrojích detailně publikována, avšak Estonsko je často uváděno jako příklad země, kde digitalizace a cloudová infrastruktura přinesly významné snížení nákladů na provoz veřejné správy[16].

Tyto zdroje poskytují podrobný pohled na ekonomické přínosy severního modelu cloudové digitalizace a jsou vhodné pro hlubší analýzu nebo citace v odborné práci.

2.1.2 Konzervativní hybrid: Německo a Francie

(více detailů obsahuje kapitola 3.2 Konzervativní hybrid)

Federovaná struktura a zachování autonomie

Německo a Francie představují konzervativní hybridní přístup charakterizovaný federovanou strukturou a zachováním významné autonomie jednotlivých úrovní veřejné správy. Tato decentralizovaná struktura vede k rozdělení provozu informačních systémů veřejné správy mezi federální úroveň, spolkové země či departementy a samosprávy na nižších úrovních.

V Německu federální vláda prostřednictvím Spolkového ministerstva vnitra (BMI) provozuje federální cloud (Bundescloud) spravovaný Spolkovým úřadem pro IT služby (ITZBund). Jednotlivé spolkové země (Länder) mají svá vlastní datová centra a cloudové služby – například konsorcium Dataport pro severoněmecké země (Šlesvicko-Holštýnsko, Hamburk, Brémy) a IT Baden-Württemberg pro stejnojmennou zemi. Města a obce si pak často udržují vlastní on-premise servery nebo uzavírají smlouvy na cloudové služby s komerčními poskytovateli. Rozhodnutí o tom, zda migrovat do spolkového cloudu, zemského cloudu, některého certifikovaného komerčního cloudu či zůstat on-premise, závisí na pravomocích a rozpočtových pravidlech jednotlivých územních celků.

Ve Francii centrální koordinaci digitalizace zajišťuje Direction interministérielle du numérique (DINUM), která schvaluje a prosazuje framework Nuage de Confiance. V jeho rámci vznikl **Bleu**, suverénní cloud provozovaný konsorciem Orange/Capgemini/Microsoft a **S3NS**, platforma Thales ve spolupráci s Google Cloud.

Francouzská ministerstva a ústřední orgány tyto suverénní cloudy využívají pro kritické a citlivé systémy. Départements a velké metropolitní oblasti si často zřizují vlastní OpenStack-based clustery označované jako Nubo, zatímco menší obce a města využívají cloudové služby velkých komerčních operátorů (např. Orange Business, SFR). I zde má každá entita značnou autonomii: výběr mezi státními cloudy, regionálními řešeními nebo komerčními službami se řídí místními potřebami, kompetencemi a rozpočtovými limity.

Certifikační rámce jako základ bezpečnosti

Obě země zavázaly veřejnou správu k využívání pouze cloudových služeb splňujících národní bezpečnostní standardy. Německo vyvinulo **BSI C5** (Cloud Computing Compliance Controls Catalog) definovaný BSI, který obsahuje 114 požadavků napříč 17 doménami včetně organizace bezpečnosti, fyzické bezpečnosti a ochrany dat. Tento standard je auditován u poskytovatelů podle ISAE 3000 a jeho využití je povinné pro federální úřady a organizace pracující s citlivými daty[17]. Od července 2025 je pro poskytovatele vyžadován audit Type 2 ověřující efektivnost kontrol po dobu minimálně šest měsíců.

Francie vyvíjí certifikační rámec SecNumCloud (ANSSI) od roku 2013. Verze 3.2 z roku 2022 klade důraz na právní suverenitu zahrnující imunitu vůči mimo-EU zákonům jako je Cloud Act, dále na evropské vlastnictví, lokalizaci dat ve Francii nebo EU a řadu technických požadavků[18]. Tento národní

[16] Estonská vláda, "Digital Estonia 2024", 2024 (https://riigikantselei.ee/digital-estonia-2024)

[17] https://aws.amazon.com/compliance/bsi-c5/

[18] https://38northsecurity.com/security-compliance/global/french-secnumcloud/

referenční rámec je používán pro veřejné zakázky a provoz operátorů důležitých služeb, přičemž kvalifikace platí tři roky a je vyžadována pro kritické systémy veřejné správy (SecNumCloud je *povinně* vyžadován pouze pro informační systémy státní správy zařazené do politiky „cloud au centre“ (citlivé IS státu)[19]. Pro ostatní kategorie citlivých či kritických systémů je jeho využití buď silně doporučeno, nebo ponecháno na rozhodnutí dané organizace po dané analýze rizik).

Financování a podpora migrace

Zajištění investic do digitalizace a migrace klíčových agend se řeší kombinací fondů, dotací a centralizovaných nákupních struktur. Německo využívá Fond Digitalisierung Haushalt s objemem 1,5 miliardy EUR pro období 2023-2027, který částečně kryje investice do spolkového gov-cloudu. Spolkové úřady platí za gov-cloud 0,28% ročního rozpočtu plus provozní náklady podle spotřeby, zatímco spolkové země spoléhají na vlastní investiční programy a rámcové smlouvy s regionálními datacentry.

Francie implementuje "Plan de relance" s objemem 750 milionů EUR pro období 2021-2025, který podporuje přechod ministerstev do SecNumCloud. Program **Plug-and-cloud** s rozpočtem 3,5 milionu EUR pomáhá startupům a malým a středním podnikům při přípravě na SecNumCloud kvalifikaci, financuje předběžné audity a konzultace. Obce dostávají dotace až 70% uznatelných nákladů na migraci kritických agend jako matrika a registr obyvatel.

Participace v evropských iniciativách

Německo a Francie aktivně participují na evropských iniciativách pro sdílení kapacit a standardizaci, zejména v rámci **GAIA-X** jako federovaného ekosystému datových prostorů. Obě země podporují use-case projekty v oblastech mobility, vzdělávání a zdravotnictví pro veřejný sektor. Cílem je zavedení společných služeb identity, katalogů API a regulačních rámců pro suverénní datovou výměnu napříč EU.

GAIA-X Hub Germany spravuje 11 projektů financovaných BMWK, včetně datového prostoru pro školství a mobility. Francie se zaměřuje na interoperabilitu zdravotnických dat a regionální smart-city projekty v rámci své participace v GAIA-X.

Na druhé straně je však třeba uvést, že relativně široce a ambiciózně pojatá strategie GAIA-X od r. 2020 zatím nepřinesla významnější využití za účelem federace a jednotné správy kapacit státních, akademických, nebo privátních cloudových poskytovatelů napříč EU. V reakci na to Evropská komise v roce 2024 spustila praktičtější pilotní iniciativu „EuroCloud“ [20] (pracovní název), založenou na standardizačním projektu SIMPL[21] (Standardized Interoperability Model for Public-private Linkages). V této nové fázi působí Německo a Francie opět jako přední lídři, přičemž se zaměřují na rychlou implementaci konkrétních technických standardů a provozních pokynů napříč veřejným a soukromým sektorem.

Úspory nákladů v konzervativním hybridu

Německo podle odhadů může přesunem 10% stávajících IT systémů veřejné správy do cloudu přinést německým daňovým poplatníkům roční úsporu přes 230 milionů EUR[22] - Simulační scénář srovnával průměrné provozní výdaje 32 federálních a zemských IT-služebních center s ekvivalentními náklady

[19] https://www.ssi.gouv.fr/administration/guide/secnumnud-cloud-referentiel-de-certification-pour-les-services-de-confiance-en-cloud/

[20] https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

[21] https://digital-strategy.ec.europa.eu/en/policies/simpl

[22] WIK-Diskussionsbeitrag Nr. 529 „Cloud-Lösungen für die öffentliche Verwaltung“ (12/2024) (https://awsdigitaldecade.publicfirst.co.uk/germany/?lang=de)

v multicloudu; úspory pocházejí z nižších licenčních poplatků, konsolidace datacenter a nižší spotřeby energie.

Další studie[23] uvádí, že efektivní cloud-cost management ve veřejné správě může vést až k 150 milionům EUR ročně v úsporách díky centralizaci, škálovatelnosti a standardizaci služeb. Studie kvantifikovala rozdíl mezi fakturovanými objemy služeb IaaS/PaaS a měřenou reálnou zátěží u 56 organizací. Úspory vyplývají z průběžné optimalizace rezervovaných instancí, vypínání nevyužitých prostředků a sjednocení nákupních rámců. Německá vládní cloudová strategie zdůrazňuje přínosy v podobě vyšší efektivity, snížení nákladů na údržbu a provoz, lepší vyjednávací pozice vůči dodavatelům a možnost sdílení infrastruktury mezi úřady.

Poznámka: Některé studie zároveň upozorňují na přechodné náklady spojené se změnou poskytovatele cloudu, které mohou v krátkodobém horizontu dosáhnout až 120 milionů EUR[24], zejména kvůli licenčním poplatkům a migraci dat. Ve 46% sledovaných případů bylo nutné nakoupit nové perpetual licence po přesunu na jinou platformu; v souhrnu 27–120 mil. EUR ročně. Tyto studie však vycházely ze stavu před přijetím Data Actu, kdy byly poplatky za migraci a licenční náklady běžné. Nově však bude většina těchto nákladů eliminována nebo zásadně omezena[25][26]. Přechod mezi poskytovateli bude pro veřejnou správu i soukromé zákazníky výrazně snazší, rychlejší a levnější.

Francie podle zprávy EY může prostřednictvím digitalizace státní správy včetně masivního přechodu na cloud dosáhnout roční úspory až 12 miliard EUR během pěti let[27]. Tato částka zahrnuje nejen úspory na IT, ale i širší efekty digitalizace veřejných služeb. Francouzská strategie "cloud first" předpokládá snížení provozních nákladů díky konsolidaci datových center, rychlejší implementaci služeb a větší flexibilitě.

2.1.3 Transformační model: Itálie

(více detailů obsahuje kapitola 3.3 Transformační model)

Centralizovaný plán masové migrace

Itálie představuje nejambicióznější transformační model s cílem migrovat do konce roku 2026 minimálně 75% systémů centrálních i lokálních orgánů (včetně škol a zdravotnických zařízení) do Polo Strategico Nazionale (PSN) nebo do jiných certifikovaných veřejných cloudů[28][29]. PSN je vládou řízená federovaná infrastruktura určená k provozu kritických a strategických agend se zárukami vysoké dostupnosti, šifrování a suverénní správy dat. Alternativou k PSN jsou cloudové služby uvedené v centrálním katalogu certificati cloud, které prošly schválením AgID podle Linee Guida Cloud. Migrační povinnost se týká centrálních i lokálních úřadů, včetně zdravotnických zařízení a škol.

Podrobnější plán italské migrace je uveden v kapitole 2.2.3. Migrační plán italské veřejné správy do PSN/kvalifikovaných cloudů.

---

[23] Lünendonk-studie „Cloud-Transformation im öffentlichen Sektor“ (04/2025), kap. „Cloud-Kostenmanagement“ (https://www.datagroup.de/wp-content/uploads/2021/08/LUE_IT_Studie-2021_DATAGROUP.pdf)

[24] ZNT Quadriga-Studie „Fair Software Licensing & Cloud in öffentlichen Unternehmen“ (02/2025) (https://themunicheye.com/Public-Sector-Cloud-Transition-Could-Cost-Up-to-EUR120-Million-11298)

[25] https://www.steel-eye.com/news/data-ownership-the-end-of-extraction-fees-eu-data-act-mandates-freedom-for-your-archives-part-2

[26] https://www.fivetran.com/blog/know-your-rights-you-can-control-extract-and-move-your-data

[27] EY Rapport« Moderniser l’État par le numérique » (2024) (https://digitales.hessen.de/sites/digitales.hessen.de/files/2022-04/nachhaltigkeitsstudie.pdf)

[28] https://www.trade.gov/market-intelligence/italy-information-technology-national-strategic-hub-cloud-services

[29] https://lucianocastro.com/en/national-strategic-pole-10-answers-on-psn/

Standardizovaná metodika migrace

Každá instituce musí projít standardizovaným procesem zahrnujícím detailní inventarizaci svých dat a aplikací s následnou klasifikací podle citlivosti na běžná, kritická a strategická data. Na základě jednotné metodiky EMG2C (Explore, Make, Go-to-Cloud) je povinností každé instituce připravit a předložit migrační plán stanovující harmonogram, odpovědnosti a způsob migrace jednotlivých systémů. Migrační plán je schvalován centrálními orgány AgID a ACN, které zajišťují jeho soulad s národní cloudovou strategií a bezpečnostními požadavky[30]. Tento centrálně koordinovaný model zajišťuje, že migrace postupuje rychle, jednotně a pod dohledem jediného regulátora, což minimalizuje duplicitní investice, zvyšuje interoperabilitu napříč správními úrovněmi a zaručuje splnění bezpečnostních a compliance standardů.

Rozsáhlá finanční podpora

Klíčovým zdrojem financování je Plán národního oživení a odolnosti (PNRR), který na digitalizaci veřejné správy a migraci do cloudu vyčlenil více než 900 milionů EUR[31]. Veřejná správa platí PSN adresně dle skutečné spotřeby služeb. Ceny jsou pevně definovány ve veřejném cenovém katalogu (Listino Servizi PSN[32]), zajišťující transparentnost a stabilitu rozpočtových výdajů. Investiční a migrační náklady mohou být plně nebo částečně hrazené z PNRR, včetně školení a programového řízení (např. AgID a DTD). PA (Pubblica Amministrazione/ veřejná správa) nevyužívají služby PSN zdarma, ale platí dle spotřeby, avšak mohou být podpořeny formou grantového financování migračních a transformačních nákladů. Část centrálních prostředků je určena na školení zaměstnanců a metodickou podporu během migrace, včetně konzultačních služeb a technické asistence.

Centralizovaná governance a koordinace

AgID (Agenzia per l'Italia Digitale) odpovídá za koordinaci digitální transformace, vydávání metodik, certifikaci cloudových poskytovatelů a dohled nad plněním migračních plánů. ACN (Agenzia per la Cybersicurezza Nazionale) stanovuje bezpečnostní standardy, posuzuje rizika a dohlíží na ochranu dat během i po migraci. Obě agentury pravidelně monitorují pokrok, vyhodnocují splnění milníků a poskytují zpětnou vazbu jednotlivým institucím.

Úspory nákladů v transformačním modelu

Transformační přechod italské veřejné správy na cloud prostřednictvím strategie Cloud Italia a infrastruktury Polo Strategico Nazionale má podle dostupných studií potenciál každoročně snižovat provozní náklady obcí zhruba o 900 milionů EUR[33] a přinášet regionálním samosprávám úsporu okolo 275 milionů EUR ročně. Při celostátní konsolidaci datových center lze ušetřit až 5,6 miliardy EUR během prvních pěti let.

2.1.4 Britský přístup: Cloud First strategie

Spojené království uplatňuje centrální Cloud First přístup podporovaný specializovanými nástroji, konsolidací datových center a robustní governance architekturou. Od roku 2013 je pro centrální vládu povinné uvažovat při každé nové či stávající IT službě nejprve o public cloudu, přičemž jiné modely jsou akceptovány jen při jasně odůvodněné nemožnosti nasazení public cloudu.

[30] https://www.agid.gov.it/en/news/agid-joins-polo-strategico-nazionale-further-step-cloud-italia-strategy

[31] https://www.italiadomani.gov.it/en/Interventi/investimenti/infrastrutture-digitali.html

[32] https://www.polostrategiconazionale.it/media/news/psn-integra-il-listino-servizi-2025-nuove-soluzioni-innovative-per-la-digitalizzazione-delle-pa-psn/

[33] AWS Public Sector Blog, 2022 (https://aws.amazon.com/blogs/publicsector/the-impact-of-the-cloud-on-the-public-administration-in-italy/)

Úspory nákladů

G-Cloud procurement framework umožňuje nákup služeb IaaS, PaaS, SaaS a podpůrných služeb bez tendru prostřednictvím Digital Marketplace s jednotnými rámcovými smlouvami a self-certifikací dodavatelů. Pravidelné iterace zajišťují otevřený přístup pro dodavatele, přičemž kontrakty mohou být uzavřeny maximálně na 24 měsíců, což minimalizuje vendor lock-in a podporuje rychlou změnu poskytovatele.

Od roku 2011 Spojené království konsoliduje stovky vládních datových center s cílem zvýšit využití serverů z přibližně 10% na 60-80% a dosáhnout ročních úspor desítek milionů liber[34]. Crown Hosting Data Centres jako joint venture Cabinet Office a Ark Data Centres nabízí hybridní cloud pro úřady, pokud nelze použít public cloud[35][36].

Rozdíl v „cloud-first" strategiích

Zatímco většina evropských zemí má **doporučující nebo hybridní přístupy**, britská strategie je mandatorní - veřejné organizace musí uvažovat public cloud jako první volbu před jakoukoliv alternativou.

Neexistuje zatím žádné závazné unijní nařízení, které by všem veřejným zadavatelům členských států přikazovalo „cloud-first" obdobně přísně jako britská politika. EU se blíží k takové úpravě – návrh Cloud and AI Development Act a připravovaný Cloud Rulebook mohou zavést „cloud-first" princip do jednotné politiky veřejných zakázek, ale legislativní proces není ukončen a text ohlášené cloudové politiky je zatím stále ve fázi příprav. Současná unijní legislativa (Data Act, NIS 2, chystaná certifikační schémata EUCS) spíše usnadňuje a reguluje používání cloudu (bezpečnost, interoperabilita, switching), ale neukládá povinnost ho povinně zvolit.

2.1.5 Srovnání české situace s implementací cloudu ve veřejné správě v evropských zemích

Rozdíly v přístupu a celkové strategii

Česká republika se v oblasti plánování přechodu na využívání cloudových služeb ve veřejné správě řídí poněkud volnějšími pravidly než většina zemí, prezentovaných v analýze výše. Podobnost lze však nalézt v existenci centralizovaného katalogu cloud computingu a související legislativy: v Dánsku a Estonsku rovněž existuje federovaně či centrálně koordinovaný katalog schválených cloudových služeb. Dále podobně jako v uvedených zemích i v ČR platí provoz agend v režimu preference (oproti on-premise) státního cloudu pro nejcitlivější systémy a využití komerčních služeb pro ostatní úrovně, přičemž se zachovává technologická neutralita a tržní principy. Ve všech těchto federovaných či decentralizovaných modelech existují rámcové smlouvy (či katalogová evidence) s hyperscalery (AWS, Microsoft, Google) či lokálními poskytovateli, které doplňují kapacity státních poskytovatelů.

Česká republika se tak v implementaci cloudových služeb ve veřejné správě liší především tím, že neexistuje jeden závazný celostátní harmonogram nebo přímý migrační plán, který by všem úřadům určoval povinnost a konkrétní termíny pro přechod do cloudu. Digitální a informační agentura (DIA) sice vydává metodiky a koordinuje strategii rozvoje eGovernment cloudu, ale harmonogram migrace si stanovuje každý správce informačního systému veřejné správy (ISVS) sám – podle životního cyklu svých agend, obnovy infrastruktury a vlastních kapacit. Přechod je tak dobrovolný, postupný a řízený decentralizovaně, bez striktního státního časového plánu.

[34] Transforming Government Data Centres" (Cabinet Office, 2018) – https://www.gov.uk/government/publications/transforming-government-data-centres

[35] The UK Government Cloud Strategy" (GDS, 2014) (https://digital.blog.gov.uk/2014/07/10/uk-government-cloud-strategy/)

[36] Crown Hosting Data Centres – Strategic Overview" (Ark Data Centres, 2020) – https://arkdatacentres.co.uk/crown-hosting/

Centrální plán v Česku existuje například pro pilotní projekty a hlavní milníky vývoje eGovernment cloudu, které jsou zakotveny ve strategických dokumentech DIA a v požadavcích na katalog cloudových služeb, ale **plošný harmonogram migrace v českých podmínkách určuje každý úřad a instituce samostatně** podle svých potřeb a možností.

Financování a ekonomický model

V severních zemích jsou z evropských prostředků financovány investiční projekty (CAPEX) – tedy výstavba, pořízení a modernizace technické infrastruktury a klíčových digitálních kapacit na centrální a někdy i regionální úrovni. Tyto projekty zpravidla zahrnují budování cloudové architektury, datových center nebo sdílených platforem, které jsou pro veřejnou správu následně zdrojem cloudového hospodaření. Obce z těchto prostředků financují jednorázové investiční náklady související zejména s připojením ke cloudu či lokální vybavení (počítače atd.).

OPEX (provozní náklady na cloudové služby) pak financují obce a samosprávy převážně z národních rozpočtů, a to formou paušálů, předplacených služeb nebo přímých plateb za skutečně využívané zdroje – existuje výslovně vyčleněna kapitolová položka národních rozpočtů. Tyto rozpočty jsou často doplňovány z dotačních národních programů, které jsou přímo určeny na podporu digitalizace veřejné správy. Klíčové je, že tato OPEX složka je zřetelně oddělena od investičních projektů a je do ní zapojený místní rozpočet obcí/samospráv, což motivuje obce k efektivnímu hospodaření s cloudovými službami a usnadňuje úhradou dlouhodobých provozních nákladů jejich trvalé využívání.

V České republice není zaveden obdobný systém paušálních příspěvků na OPEX cloudových služeb pro obce a samosprávy. Náklady na provoz cloudových služeb si hradí každý úřad sám ze své rozpočtové kapitoly ICT, bez cílené dotační podpory nebo vyčleněné částky v rozpočtu. Zároveň neexistuje žádný celostátní grantový program, který by pravidelné poplatky za cloud kompenzoval.

Evropské fondy financují téměř výhradně investice (CAPEX) – tedy pořízení infrastruktury, hardwaru, licencí nebo systémů, nikoli dlouhodobý provoz (OPEX). Na OPEX (provoz cloudových služeb) tyto programy nepřispívají, a úřady tedy nemohou žádat o dotace na běžné měsíční/roční poplatky za cloud, byť užívají služby z Katalogu cloud computingu.

Národní dotační programy (například v gesci MMR nebo MPO) jsou rovněž zaměřeny na investiční podporu – nákup vybavení, rekonstrukce, digitalizace agend, přípravu IS – nikoli na kofinancování běžných provozních nákladů. Výsledkem je, že české úřady musí každoročně krýt OPEX cloudu z vlastních rozpočtů bez vnější podpory, což v reálné praxi snižuje motivaci k rychlejší migraci na cloudové služby oproti on-premise řešením, která lze dotovat z evropských fondů právě kvůli investičnímu charakteru.

Technologická připravenost a bezpečnostní standardy

Technologická připravenost a bezpečnostní standardy se v České republice od ostatních analyzovaných zemích příliš neliší – rozdíly jsou spíše v tom, jak jsou pojmenovány jednotlivé nástroje, jak jsou implementovány a jak silně je dodržována jednotná praxe. Oba modely vycházejí z hybridního přístupu: kritické agendy na státním cloudu, ostatní na komerčních službách splňujících bezpečnostní standardy.

Hlavní společné prvky jsou:

- Bezpečnostní standardy: všechny analyzované země (Švédsko, Dánsko, Estonsko, ČR, Německo, Francie) mají jasně definované bezpečnostní třídy nebo úrovně pro cloudové služby a vyžadují jejich použití podle citlivosti dat. Rozdíl je v počtu kategorií, jejich pojmenování a míře formálnosti certifikace, ale základní myšlenka (vyšší úroveň ochrany pro citlivější data) je ve všech případech totožná.
- Centrální katalog či rámcové smlouvy: státní autorita vede seznam schválených poskytovatelů a služeb, ze kterého úřady vybírají.

- Technologická neutralita: žádný jediný dodavatel není upřednostňován; úřady mohou vybrat vhodného hyperscalera nebo lokálního poskytovatele, pokud splňuje standardy.

Organizační struktura a governance

V České republice se na přechodu informačních systémů veřejné správy do cloudu podílí několik subjektů[37]. Tento model se podobá německému federovanému přístupu.

Na centrální úrovni je to především **Digitální a informační agentura (DIA)**. DIA koordinuje využívání cloud computingu orgány veřejné správy, vydává metodické pokyny pro využívání cloud computingu orgány veřejné správy, zpracovává plán zajištění potřebné kapacity pro poskytování cloud computingu poskytovatelem státního cloud computingu orgánům veřejné správy, včetně rozpočtového výhledu na 5 let a předkládá ho vládě, navrhuje opatření k zajištění dlouhodobě udržitelného financování využívání cloud computingu orgány veřejné správy, kontroluje, zda cloud computing poskytovaný orgánům veřejné správy splňuje požadavky podle § 6n ZoISVS a kvalitu tohoto cloud computingu,, spravuje informační systém cloud computingu pro orgány veřejné správy, vede katalog cloud computingu pro orgány veřejné správy, a dále vykonává působnost správního orgánu příslušného k uplatňování, regulaci a kontrole cen podle právního předpisu upravujícího ceny v případě cen za poskytování cloud computingu orgánům veřejné správy., zpracovává plán zajištění potřebné kapacity ve státním cloudu, vykonává působnost správního orgánu. Navíc všechny větší investice do IT schvaluje.

Národní úřad pro kybernetickou a informační bezpečnost (NUKIB) kontroluje, zda cloud computing poskytovaný orgánům veřejné správy splňuje požadavky podle § 6n, v případě, že je využíván k provozování informačního systému veřejné správy, který je informačním nebo komunikačním systémem kritické informační infrastruktury, významným informačním systémem nebo informačním systémem základní služby podle právního předpisu upravujícího kybernetickou bezpečnost.

Orgán veřejné správy může využívat pouze cloud computing, který splňuje požadavky podle § 6n a je poskytovaný poskytovatelem státního cloud computingu nebo poskytovatelem cloud computingu zapsaným v katalogu cloud computingu na základě nabídky cloud computingu tohoto poskytovatele zapsané v okamžiku jejího přijetí orgánem veřejné správy v katalogu cloud computingu, aktuálně také v rámci vertikální nebo horizontální spolupráce podle právního předpisu upravujícího zadávání veřejných zakázek nebo v rámci obecné výjimky z povinnosti zadat veřejnou zakázku v zadávacím řízení podle právního předpisu upravujícího zadávání veřejných zakázek. Další výjimky jsou definovány v §6l odst.4 ZoISVS.

Orgány veřejné správy v rozsahu své zákonné působnosti provádějí výběr technických a programových prostředků a dalších produktů pro provoz jimi vytvářených a spravovaných informačních systémů veřejné správy; to neplatí pro orgány veřejné správy, pro něž jsou závazná usnesení vlády, předpokládá-li informační koncepce České republiky užití produktu určitých vlastností. OVS jsou v rámci ISVS povinny spolupracovat s DIA, předkládat k vyjádření návrhy na pořízení, architektonické změny a investiční záměry akcí související s uvedeným. V rámci toho také musí provádět hodnocení ekonomické výhodnosti způsobu provozu jimi spravovaných systémů nebo při pořízení nového ISVS či architektonické měně.

DIA krom role metodického garantu a koordinátora cloudové migrace nyní přímo provozuje a rozvíjí: Správu základních registrů, Systém datových schránek, Portál veřejné správy (gov.cz), Portál občana (portalobcana.gov.cz), Aplikaci eDoklady a další podpůrné systémy.

37 https://digitalnicesko.gov.cz/media/files/Informa%C4%8Dn%C3%AD_koncepce_%C4%8Cesk%C3%A9_republiky_2024.docx.pdf

Současný stav digitalizace v evropském kontextu

V mezinárodním srovnání se Česká republika nachází na 20. místě z 27 zemí EU podle DESI indexu s celkovým skóre 68%[38]. Toto umístění ve spodní polovině evropského žebříčku kontrastuje s úspěchy zemí jako Estonsko, které je považováno za evropského lídra v digitalizaci veřejné správy, nebo Dánsko, kde sdílený model přinesl úspory 30-40% v celkových nákladech vlastnictví IT.

Problémem české situace je zejména nízká míra úplné digitalizace služeb ve veřejné správě[39]. Česko má největší nedostatky v oblasti předvyplněných formulářů, kde se řadí ke konci žebříčku před Německo a Rumunsko. Souvisí to se stále nedostatečným sdílením dat napříč orgány veřejné správy, na kterém v tuto chvíli veřejná správa usilovně pracuje.

V soukromém sektoru Česká republika patří k ekonomikám s poměrně rychlou digitalizací, kde podniky často předbíhají státní správu. Zatímco v podnicích s minimálně deseti zaměstnanci využívá cloudové technologie již 47% firem, což překračuje průměr EU[40], veřejná správa zaostává.

Ve spojitosti s dlouhodobě rostoucím podílem online prodejů a moderních platebních metod, které zvyšují komfort a efektivitu transakcí, patří celkově soukromý sektor ČR k nejrychleji se digitalizujícím ekonomikám v EU.

Právní rámec a regulace

Česká republika vyvinula poměrně komplexní regulatorní rámec pro cloud computing včetně povinnosti zápisu poskytovatele cloud computingu v katalogu cloud computingu a povinných certifikací pro nabídky cloud computingu poskytovatele[41]. Tento přístup je podobný francouzskému SecNumCloud systému, ale liší se od minimalistického přístupu severních zemí, které spoléhají více na důvěru a standardizaci než na detailní regulaci.

Český přístup připravuje půdu pro implementaci evropského Data Act, který od září 2025 bude vyžadovat usnadnění změny poskytovatelů cloudových služeb.

Vendor lock-in a závislost na dodavatelích

Česká veřejná správa se potýká s problémem vendor lock-in způsobeným fungováním agendových systémů z 90. let, které stále v některých resortech fungují., České úřady tak musí řešit migraci monolitických aplikací s těsnou provázaností komponent. Tato situace je podobná německé, kde federální struktura také zpomaluje centralizaci IT služeb, protože jednotlivé úrovně veřejné správy uzavíraly samostatné smlouvy bez jednotných standardů, což umožnilo „uzamčení“ některých dodavatelů.

Česká republika od počátku nasadila složité, neflexibilní a monolitické systémy bez plánované architektonické migrace a s nedostatečnou modularitou, což vedlo ke stále horší situaci. To je dáno především tím, že většina aplikací byla vyvinuta v 90. letech a nebyla postupně refaktorována nebo modernizována na otevřené standardy a mikroservisy, například na rozdíl od Estonska, Dánska či Švédska, které již od r. 2000 budovaly své systémy s ohledem na otevřenost, interoperabilitu a možnost migrace. Zjednodušeně řečeno, zatímco v ostatních zemích se v průběhu času i díky novým digitálním strategiím podařilo odsunout nebo minimalizovat riziko vendor lock-in, v ČR jsou na některých místech běžné staré, monolitické systémy, což výrazně zvyšuje složitost jejich modernizace a migrace do cloudových prostředí.

[38] https://www.businessinfo.cz/clanky/ceska-republika-si-polepsila-v-oblasti-digitalizace-sluzeb-verejne-spravy-zustava-ale-v-dolni-polovine-evropskeho-zebricku-desi/

[39] https://blog.cesko.digital/2024/10/priciny-problemu-digitalizace-verejne-spravy-v-cr

[40] https://www.czechbusinessguide.com/content-of-book-research-and-development-digital-and-innovation/

[41] https://www.mt-legal.com/pravidla-pro-vyuzivani-cloud-computingu-organy-verejne-spravy-z-pohledu-zzvz/

Dalším typickým rysem pro ČR byly nevhodné smluvní podmínky: ve smlouvách o dodávce systémů nebyla sjednána práva na zásahy či úpravy třetími osobami. Zadavatelé tak museli veškeré změny a údržbu zadávat výhradně původnímu dodavateli, který díky tomuto monopolnímu postavení mohl stanovit vysoké ceny a podmínky pro jakoukoli modifikaci, ke které také držel/drží jedinečné know-how.

2.2 Vybrané aspekty adopce cloudu v zahraničí

2.2.1 Strategie non-EU poskytovatelů cloudových služeb

Ne-EU hyperscaleři, **především američtí poskytovatelé veřejného cloudu**, reagují na zpřísňující evropskou legislativu ve spojení s tlakem národních regulatorních rámců (zejména francouzských a německých) budováním samostatných „suverénních cloudů“, které garantují kontrolu nad daty, jejich lokalizaci a soulad s právními předpisy EU.

Pro potřeby evropských organizací lze suverénní cloudy rozdělit do čtyř úrovní podle míry kontroly nad zpracováním a ukládáním dat, geografického omezení provozu, personálních podmínek a vhodnosti pro různé kategorie systémů:

Stupeň 1 – Základní suverenita

V této úrovni se zákazníkům garantuje uložení neaktivních dat („data at rest“) v rámci zemí EU, přičemž dočasné zpracování dat při provádění jistých úloh (služeb) může nastat i v globálních regionech mimo EU, včetně USA. Primární operace probíhají v EU, avšak zálohy či provozní procesy mohou využívat i zdroje z ostatních regionů, pokud existuje rozhodnutí o adekvátnosti datových přenosů (např. mezi EU a USA). Nejsou uplatňována žádná dodatečná personální omezení. Tento model je vhodný pro systémy s nízkým až středním rizikem (orientačně bezpečnostní úrovně 1–2), které chtějí plně využít platformních služeb hyperscalerů bez geografických restrikcí.

Stupeň 2 – Zesílená suverenita

Zde jsou data geofencingem omezena tak, že jak uložení neaktivních zákaznických dat, tak záložní kopie a logy jsou uloženy výhradně v EU. Přenos dat mimo hranice EU je zakázán i pro dočasné přenosy, zálohy lze replikovat pouze na dalších územích EU. Smlouvy o podpoře umožňují (zpravidla za příplatek), aby primární technická podpora a údržba byla zajištěna personálem působícím v EU. Tento model se hodí pro systémy střední citlivosti (orientačně bezpečnostní úrovně 2–3), které vyžadují vyšší kontrolu nad lokalizací dat.

Stupeň 3 – Rozšířená suverenita

Cloudové prostředí odděluje serverovou infrastrukturu poskytovatele od automatických aktualizací a systémové správy od veřejného internetu. Všechny práce na serverové infrastruktuře se musí provádět „manuálně“ off-line přenosem SW aktualizací a nových služeb do izolovaných a vymezených zón pouze v rámci EU. Přísný zákaz ukládání či zpracování dat mimo EU platí i pro záložní systémy. Všichni operátoři a údržbáři datových center musí být občané zemí EU. Tento stupeň je určen pro kritické státní aplikace, zdravotnické systémy a krizové řízení (orientačně bezpečnostní úrovně 3–4).

Stupeň 4 – Maximální suverenita

Nejvyšší úroveň, kdy je cloud plně vlastněný a provozovaný evropskými či národními subjekty s tzv. imunitou vůči žádostem o zpřístupnění zákaznických dat, pocházející od orgánů činných v trestním řízení mimo EU. Hardwarová i softwarová stopa zůstává kompletně v EU a pod přímou kontrolou odpovědných evropských orgánů. Jakékoli ukládání, zpracování či zálohování dat mimo EU je absolutně zakázáno. Veškerý personál, hardware i infrastruktura jsou pod přímou správou evropských institucí. Tento model je rezervován pro strategická data národní bezpečnosti a kritickou infrastrukturu s nejvyšším možným dopadem (orientačně bezpečnostní úroveň 4).

Příklady „Suverénní“ cloudové infrastruktury

Amazon Web Services investuje 7,8 miliardy EUR do roku 2040 do AWS European Sovereign Cloud jako samostatné infrastruktury v Brandenburgu, plně oddělené od globálních AWS regionů. Společnost založila novou německou mateřskou společnost a tři dceřiné společnosti v Německu s výhradně EU personálem kontrolujícím všechny operace a přístup k datům. Tento projekt lze zařadit do stupně 3 –

Rozšířená suverenita, jedná se stále o komerční produkt nadnárodního poskytovatele (Amazon Web Services) včetně lokalizace do EU společností.

Microsoft vyvinul Sovereign Public Cloud s rozšířenými funkcemi Data Guardian zajišťující, že veškerý vzdálený přístup k evropským datům je schvalován a monitorován evropským personálem v reálném čase[42][43]. EU Data Boundary zajišťuje kompletní lokalizaci dat Microsoft 365 a Azure v EU společně s vytvořením evropské rady ředitelů operující podle evropského práva. Tento projekt lze zařadit do stupně 2 – Zesílená suverenita, jedná se o komerční cloudovou platformu, nikoliv EU-vlastněnou instanci, avšak s posílenou kontrolou nad daty a přístupem.

Google Cloud vybudoval sovereign cloud portfolio s rozšířenými funkcemi Data Guardian prostřednictvím partnerství s evropskými společnostmi jako Thales ve Francii a T-Systems v Německu[44][45]. Google Cloud Dedicated umožňuje lokální a regionální nasazení a získal kvalifikaci SecNumCloud 3.2 ve Francii ve spolupráci s Thales (pod názvem „S3NS“), obdobně jako projekt „Bleu“ aplikující izolovanou instanci Microsoft Azure, avšak provozovanou evropskými partnery Orange a CapGemini ve Francii. Tyto projekty lze zařadit do stupně minimální 3 – Rozšířená suverenita, jedná se o izolovaně nasazenou komerční cloudovou platformu hyperscalera prostřednictvím partnerství s evropskými společnostmi.

Příkladem nejvyššího stupně 4 – Maximální suverenita jsou budované státní cloudy v části pro nejcitlivější systémy:

- „Bundescloud“ – německá federální státní cloudová platforma. Vlastnictví a provoz: platformu vyvíjí a provozuje Spolkový úřad pro IT bezpečnost (BSI) ve spolupráci se Spolkovým ministerstvem vnitra (BMI) a spolkovými datovými centry tak, aby infrastruktura byla vlastněna výlučně federálními institucemi.
- Polo Strategico Nazionale „PSN“ - celá infrastruktura („core cloud“) je ve vlastnictví AGID a provozována ve čtyřech datových centrech v regionech Lazio, Lombardia, Campania a Veneto, bez zapojení komerčních poskytovatelů. PSN provozuje kritické agendy ministerstev, finanční správy, zdravotnické registry a krizové řízení.

Vzhledem k výše uvedeným omezením hyperscaleři (a samozřejmě i další poskytovatelé cloudů včetně státních) nabízejí své „suverénní“ cloudy pod výrazně odlišnými podmínkami než zcela standardní veřejný komerční cloud, a proto by si zákazníci v EU vždy měli ověřit:

1. Ochranu proti přístupu non-EU orgánů – takový suverénní cloud musí garantovat, že data podléhají výhradně právu EU a nejsou vydatelná na základě extrateritoriálních zákonů jako americký CLOUD Act. Například Leaseweb uvádí, že ve svém evropském suverénním cloudu je veškerá správa infrastruktury, provoz a přístup vyhrazen výhradně subjektům registrovaným v EU, čímž se eliminuje riziko nuceného zpřístupnění dat neevropským orgánům[46].
2. Dostupnost platformních služeb - hyperscaleři často omezují škálu služeb ve svých suverénních (izolovaných) edicích. Například německý projekt Delos Cloud zatím neobsahuje speciální AI

[42] https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/

[43] https://techcrunch.com/2025/02/26/microsoft-finalizes-its-eu-sovereign-cloud-project/

[44] https://cpl.thalesgroup.com/blog/encryption/thales-digital-security-google-next-2025

[45] https://www.s3ns.io/en

[46] https://www.leaseweb.com/en/about-us/sovereignty

hardware ani Azure Automation, které jsou standardně dostupné ve veřejném Azure, a některé pokročilé databázové či analytické funkce jsou zpočátku vynechané[47].

3. Cenová politika a příplatek - suverénní cloudy bývají dražší než ekvivalentní veřejný cloud. Delos udává, že průměrný příplatek proti standardní public cloud nabídce Microsoftu se pohybuje kolem 15%. Zákazníci by si měli nechat předložit detailní ceník a vyčíslit, o kolik procent se jejich faktura zvýší oproti obyčejnému veřejnému cloudu.

Pouze na základě těchto informací (právní podmínky, rozsah služeb, cenový příplatek) lze kvalifikovaně rozhodnout, zda je konkrétní suverénní cloudová nabídka vhodná pro daný informační systém požadované úrovně zabezpečení.

Logicky odtud vyplývá, že státní cloudy budou patřit mezi nejdražší poskytovatele, a to přestože jsou jejich služby relativně omezené. To platí i pro státní část českého eGovernment cloudu (SeGC).

2.2.2 Estonské datové velvyslanectví

Estonsko vyvinulo unikátní řešení pro zajištění kontinuity svých digitálních služeb prostřednictvím světově prvního "datového velvyslanectví" v Lucembursku[48]. Toto inovativní řešení kombinuje vysokou technickou bezpečnost s diplomatickou imunitou a plnou estonskou suverenitou nad daty.

Datové velvyslanectví je umístěno v datacentru v Betzdorfu ve východním Lucembursku s bezpečnostní certifikací Tier 4, což představuje nejvyšší úroveň pro datová zařízení. Provozováno je LuxConnect's Tier IV datacentrem v Bissen s využitím Microsoft Azure pro virtuální velvyslanecké řešení.

Smlouva byla podepsána 20. června 2017 mezi premiéry Jüri Ratasem a Xavierem Bettelem a schválena estonským parlamentem 22. března 2018 [19][49]. Datové velvyslanectví má stejnou imunitu jako fyzické velvyslanectví podle Vídeňské úmluvy o diplomatických stycích s daty plně pod estonskou kontrolou a jurisdikcí.

V Lucembursku je zálohováno deset strategických databází zahrnujících elektronický pozemkový registr, registr daňových poplatníků, obchodní registr, registr obyvatelstva, státní věstník, registr identitních dokumentů, katastr nemovitostí a registr národního důchodového pojištění. Obsah datového velvyslanectví je průběžně aktualizován s různou frekvencí podle potřeb jednotlivých databází.

Řešení v podobě datového velvyslanectví formou co-location datového centra v jiné zemi EU však nemá za cíl vytvořit záložní kapacitu pro veškeré potřeby cloudových služeb v Estonsku. Jedná se o strategickou zálohu funkce kritických systémů a datových registrů pro případ rychlého obsazení této malé země v ohroženém teritoriu.

2.2.3 Migrační plán italské veřejné správy do cloudu PSN nebo do kvalifikovaných komerčních cloudů

Následující souvislý popis zachycuje jednotlivé fáze, klíčové kroky i principy metodiky EMG2C[50]:

Italská cloudová transformace běží **ve třech po sobě jdoucích etapách**. **V první**, přípravné fázi v roce 2021 byly nejprve vyhlášeny tendry na vybudování čtyř georedundantních datových center PSN. Současně vstoupila v platnost novela tzv. „Cloud First“ reformy (M1C1-2), která stanovila, že každá veřejná instituce je povinna nejprve zvažovat cloudové řešení. V rámci Přípravné fáze proběhla také

[47] https://www.heise.de/en/news/Delos-Sovereign-cloud-10-to-20-more-expensive-than-Microsoft-s-public-cloud-10102043.html

[48] https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/

[49] https://opensourcelab.dfki.de/the-cyber-state-opens-the-worlds-first-cyber-embassy/

[50] https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/

povinná inventarizace („cenzus“): každý správní celek zmapoval všechna svá datová úložiště, aplikace i služby a klasifikoval je dle citlivosti na strategická, kritická a obyčejná data.

Druhá etapa, nazvaná Implementace PSN, probíhala v průběhu roku 2022. Do konce čtvrtého čtvrtletí 2022 byly dokončeny fyzické a síťové instalace PSN, kvalifikováni první poskytovatelé cloudových služeb podle standardů Agenzia per la Cybersicurezza Nazionale (ACN) a zahájena pilotní migrace vybraných ústředních správních úřadů a zdravotnických institucí.

Následovala třetí, masová migrační fáze plánovaná na roky 2022–2026. Plán předpokládá, že do roku 2024 migruje do PSN nebo do kvalifikovaných komerčních cloudů všech 100% ústředních veřejných administrativ a lokálních zdravotnických úřadů a že k roku 2026 dosáhne migrace minimálně 75% všech subjektů veřejné správy. Migrace se řídí jednotnou metodikou EMG2C (Explore, Make, Go-to-Cloud). Nejprve (Explore) probíhá hloubková analýza stávajících systémů, identifikace závislostí a rizik. Následně (Make) se zřizuje cloudové prostředí, zabezpečují se datové toky a nastavují bezpečnostní a compliance mechanismy. V poslední fázi (Go-to-Cloud) dochází k vlastnímu přechodu, aktivaci služeb, nepřetržitému monitoringu a následné optimalizaci výkonu.

Vysvětlení šíře nabídek a role správce cloudu PSN (Polo Strategico Nazionale (PSN) PSN je realizováno prostřednictvím společnosti Polo Strategico Nazionale S.p.A., která je vlastněna konsorciem čtyř klíčových subjektů:

- TIM (45%) - hlavní italský telekomunikační operátor
- Leonardo (25%) - obranný a technologický koncern
- CDP Equity (20%) - investiční rameno státní Cassa Depositi e Prestiti
- Sogei (10%) - státní IT společnost Tato společnost provozuje datacentra PSN, koordinuje infrastrukturu a službu[51].

PSN Spa má **koncesi na 13 let** a služby každému orgánu veřejné správy musí poskytovat nejméně 10 let od migrace[52].

PSN Spa zajišťuje hosting v datacentrech v *Lombardii (Rozzano, Santo Stefano Ticino)* a *Lazio (Acilia, Pomezia)*. Infrastruktura je navržena v dual-region a dual-AZ konfiguraci pro zajištění vysoké dostupnosti a disaster recovery. Datová centra splňují nejvyšší standardy včetně **Tier IV and ANSI/TIA 942 Rating 4** a **mezinárodní certifikace,** jako jsou ISO 50001, ISO 14001, and LEED Gold.[53].

Výstavba PSN zahrnuje také konsolidaci IT center centrálních, regionálních i některých místních úřadů. Datacentra samospráv a regionů jsou integrována do PSN prostřednictvím koncesní infrastruktury; Pay-per-use model podporuje migrace v režii PSN Spa a doprovodných smluv. Není to jen federace IT center, ale centrálně spravované prostředí.

Tabulka 1 – Rozdělení služeb PSN[54]

Druhy služeb, poskytované prostřednictvím PSN Spa:	Poskytovatelé, zapojení do PSN	Poznámka
Vlastní datacentra PSN	PSN Spa (TIM, Leonardo, CDP, Sogei)	Spravuje fyzická DC, zajišťuje centralizaci správy služeb

[51] https://focus.namirial.it/psn-polo-strategico-nazionale-cose-come-funziona-2/

[52] https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/

[53] https://www.wired.it/cloud-polo-strategico-nazionale-servizi-microsoft-google-oracle-bandi-gare/

[54] https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/

Public Cloud PSN Managed	Oracle Alloy, Google Assured Workload,	Hostované v datacentrech PSN nebo v italských regionech, na fyzicky oddělené HW infrastruktuře, a spravované PSN Spa.
Hybrid Cloud on PSN site	Microsoft Azure	Cloud privátní + Azure hybrid integrace přes Azure Arc; vývoj a správa probíhá přes Azure Control Plane, přičemž data zůstávají na území Itálie
Secure Public Cloud	Microsoft Azure, Google Cloud, AWS	Datová centra v Itálii, s PSN spravovaným šifrováním klíčů, izolací dat a s možným využitím Confidential Computing.

Strategická úroveň dat musí běžet jen na privátní části cloudu (vlastní datacentra) PSN Spa.

Kritická úroveň dat musí běžet na některé ze služeb v rámci nabídky PSN Spa v tabulce výše (Encrypted Public Cloud, Licensed Private/Hybrid Cloud)[55]

Běžná úroveň dat smí využívat služeb schválených (Qualified) komerčních cloudů za podmínek jistých bezpečnostních opatření, nebo může využívat některé z nabídek PSN Spa v tabulce výše.

Governance celého procesu zajišťují tři instituce:

- AgID stanovuje technické standardy a interoperabilitu,
- ACN dohlíží na kyberbezpečnostní požadavky a
- DTD (Ministerstvo technologické inovace) koordinuje harmonogramy, schvalování migračních plánů a monitoring plnění milníků.

Každý plán musí být schválen ACN i DTD a certifikován podle národní legislativy. Tím se zaručuje jednotný přístup napříč všemi úřady a transparentní sledování úspěšnosti migrace.

Tento strukturovaný postup, podpořený legislativním mandátem „Cloud First“ a robustním finančním rámcem PNRR (900 mil. EUR), umožní Itálii dosáhnout vysoké míry cloudové adopce, zvýšit efektivitu i bezpečnost státních systémů a minimalizovat vendor lock-in při zachování kontroly nad strategickými daty.

2.2.4 Principy dánského finančního modelu ve veřejné správě

Jedná se o příklad financování ze Severního modelu.

Financování cloudových služeb v dánské samosprávě uplatňuje efektivní sdílení nákladů, spravedlivé rozdělení finanční zátěže a motivaci k udržitelné digitalizaci.

Dánské municipality se od roku 2010 postavily proti privatizaci tehdy de facto monopolního poskytovatele aplikací a sdílených služeb KMD A/S, a jako reakci na zvyšování cen za strany KMD A/S iniciovaly prostřednictvím své asociace KL – Kommunernes Landsforening založení účelové neziskové organizace KOMBIT, která měla vytvořit konkurenci vůči KMD A/S.

Výhodou Dánska je také koncentrace obcí do 98 „City Councils“, které jsou více srovnatelné svojí velikostí a snáze přijímají společná rozhodnutí. KOMBIT se proto zaměřil primárně na vlastní vývoj a alternativní poskytování agendových aplikací na modulární bázi a s otevřenými rozhraními. Jednotlivé „city councils“ participují na celkových nákladech provozu aplikací u KOMBIT podle předem dohodnutých pravidel, a to vždy tak, aby daná finanční participace byla co nejvíce spravedlivá vzhledem k charakteru poskytované aplikace. Tato participace je u plošně využívaných služeb (např. sociální

[55] https://docs.italia.it/media/pdf/italian-cloud-strategy-docs/stabile/italian-cloud-strategy-docs.pdf

služby, školství) odvozena od počtu obyvatel; v případě interních provozních aplikací je odvozena od počtu aktivních uživatelů (úředníků); v případě silně modulárních systémů (např. HR) je odvozena od rozsahu využívaných modulů daného systému.

Jednotlivé obce mají podporu v nástroji „KLIK“, který pomáhá obcím sledovat, jaké služby využívají, v jakém rozsahu, a jaké náklady s tím souvisejí. KOMBIT je hlavně v oblasti provozních IS trvale v konkurenci s KMD A/S, který nadále nabízí veřejné správě zejména horizontální IS, např. ekonomické agendy KMD Opus, využívající SAP S/4HANA Cloud na Microsoft Azure, správu dokumentů KMD WorkZone na Oracle Exadata Cloud, dále KMD Payment Hub nebo KMD Energy Management. Tato konkurence zajišťuje dlouhodobě výhodné ceny pro dánské municipality, které mohou pro jednotlivé IS samostatně hodnotit výhodnost nabídek KOMBIT nebo KMD A/S.

Centralizované nákupy zajišťuje KOMBIT jako kupní jednotka, která vyjednává rámcové smlouvy na licence, hardware i služby pro všechny obce. Sdílené zakázky přinášejí úspory z rozsahu až 28% oproti individuálním nákupům a eliminují duplicitní infrastrukturu i potřebu opakovat vlastní vyjednávání o cenách. Asociace Local Government Denmark (KL) se omezuje na koordinaci požadavků obcí a zastupování obcí v projednávání u KOMBIT

Financování dánských municipalit se opírá o kombinaci místních daní z příjmu (asi 71% rozpočtu), blokových grantů od státu (cca 26%) a uživatelských poplatků za specifické služby. Tento mix zdrojů dává obcím dostatečnou flexibilitu při nastavení daňových sazeb v rámci zákonných limitů, přičemž státní příspěvky garantují dostupnost základních funkcí.

Rizika spojená s vývojem a implementací IT systémů nese centrálně KOMBIT: obce začínají platit až poté, co řešení funguje podle stanovených parametrů, a úhrady jsou rozloženy postupně. Tím se minimalizuje finanční expozice jednotlivých obcí a zároveň se podporuje kvalita dodávaných řešení.

Generované úspory se reinvestují do dalšího rozvoje digitálních služeb, školení zaměstnanců i modernizace infrastruktury. Do roku 2020 přispěla digitalizace podle odhadů k ročním úsporám ve výši až 3 miliard DKK, přičemž samotný program základních dat šetřil dalších 250 milionů DKK ročně a dánský soukromý sektor těžil z přínosů ve výši 500 milionů DKK každoročně.

Celkově spojuje dánský finanční model udržitelné rozdělení nákladů, motivaci ke kvalitě a sdílení zdrojů tak, aby i malé obce měly přístup k moderním IT službám, a zároveň vytváří prostor pro stálé zlepšování a inovace.

2.3 Celkové náklady vlastnictví (TCO)

Evropské vlády používají metodu TCO především k porovnání krátkodobých investic do cloudu s dlouhodobými provozními výdaji stávajících systémů. Přesto se s ní nakládá rozdílně podle čtyř sledovaných modelů.

1. **Severní model (Švédsko, Dánsko, Estonsko) -** TCO se zde zohledňuje už při uzavírání rámcových smluv. Dánské obce platí za základní služby podle přesně definovaných klíčů (populace, uživatelé, moduly) a šetří tak v průměru 25 - 30% proti individuálním nákupům, protože do TCO vstupují i sdílené náklady na provoz, energii či licenční maintenance[56]. V Estonsku se TCO cloudových služeb řídí centralizovaným státním cloudem e-Cloud a platformou X-Road, jejichž režijní náklady (provoz, údržba, zálohování, energie) se hradí z centrálního rozpočtu. Penetrační testy a audity jsou zahrnuty v běžné údržbě RIA, nikoli jako zvláštní TCO položka.[57].
2. **Konzervativní hybrid (Německo, Francie) –** TCO je využíváno jako interní nástroj pro ekonomické hodnocení. Součástí jsou legislativní náklady na compliance, revize kódů a periodické audity[58]. Integruje se do strategie cloud-first a dlouhodobého plánování IT, kdy TCO pomáhá vyvážit požadavky na bezpečnost a suverenitu s ekonomickou efektivitou. Výsledky TCO analýz se používají při interním schvalování rozpočtů federálních či regionálních úřadů a podpoře obchodních případů (business cases) pro migraci kritických aplikací do certifikovaných cloudů.
3. **Transformační model (Itálie, PSN) – PSN v rámci „Explore“ fáze EMG2C** zakotvila povinné TCO; každý migrační plán musí obsahovat srovnání nákladů status quo a pěti let provozu v PSN. Do bilance se započítávají i školení, licence SaaS, poplatky za datové egress a budoucí náklady na *exit strategy*. PSN uvádí, že centralizace správy datových center povedou k významným úsporám veřejných výdajů, a to díky uzavření neefektivních menších datových center a náhradě moderní, energeticky úspornou infrastrukturou PSN.[59].
4. **Cloud-first model (Spojené království) -** G-Cloud vyžaduje, aby každý úřad před uzavřením kontraktu zpracoval business case, který obsahuje odhad nákladů na využití vybraných služeb a srovnání s on-premise řešením. Uvádí se, že srovnáním TCO on-premise a využití služeb cloudu se dosáhlo 34% provozních úspor[60].

2.3.1 Možné nedostatky zpracování při využití standardního TCO přístupu

Zpracování konvenční TCO analýzy se soustředí především na kapitálové (CAPEX) a provozní (OPEX) výdaje spojené se servery, sítí a licencemi, avšak často nevěnují pozornost následujícím klíčovým položkám, které by měly být dle metodiky zohledněny[61]:

1. Migrační náklady
   a) **Refaktoring aplikací** - úprava legacy systémů pro cloudový provoz (kontainery, micro-services) vyžaduje investice do architektů a vývojářů, často v řádu stovek tisíc eur na jeden větší modul.
   b) **Paralelní provoz (dual-run)** - během migrace běží staré i nové prostředí zároveň, což zdvojnásobuje některé náklady na dobu 3–12 měsíců.

[56] https://en.digst.dk/media/mndfou2j/national-strategy-for-digitalisation-together-in-the-digital-development.pdf

[57] https://e-estonia.com/estonia-100-digital-government-services/

[58] https://www.pwc.de/en/digitale-transformation/bsi-c5-german-bsi-catalogue-of-requirements-for-more-transparency-in-the-cloud.html

[59] https://www.wanclouds.net/blog/migration-as-a-service/the-hidden-costs-of-on-prem-to-cloud-migration

[60] https://www.wipro.com/applications/calculate-the-tco-savings-of-moving-to-oracle-cloud-infrastructure/

[61] https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/metodiky-navody-formulare/metodika-tco-metodika-pro-vypocet-celkovych-nakladu-vlastnictvi-isvs

2. Compliance požadavky
    a) **Legislativní audity a certifikace** - splnění požadavků GDPR, NIS 2 a národních norem generuje náklady na externí auditní firmy i interní právní a technické týmy.
    b) **Pravidelné recertifikace** - obnovení certifikací každé 2–3 roky znamená další jednotky set tisíc eur v auditních poplatcích.
3. Rizikové faktory
    a) **Vendor-lock-in** - překvalifikace odborníků a přepis částí systému či infrastruktury při změně poskytovatele může stát 10–20% původního rozpočtu. To platí pro on-premise i cloud.
    b) **Kybernetické incidenty** - odhadované náklady na reakci a nápravu po úniku dat u veřejné instituce se pohybují v desítkách milionů eur, plus skrytá reputační ztráta.
4. Strategické přínosy (intangible benefits)
    a) **Business agility** - rychlé prototypování a zkrácení time-to-market o desítky procent zvyšuje příjmy či snižuje provozní rizika – klasické TCO jej neoceňuje.
    b) **Uživatelská spokojenost** - lepší dostupnost a výkon e-služeb vede k úspoře pracovního času občanů i úředníků, ale tyto „sociální přínosy“ zůstávají podhodnocené.
    c) **Environmentální dopady** - snížení energetické stopy cloudem oproti on-premise datacentrům může představovat významné externí úspory za emise CO_2, avšak tradiční účetní bilance je nezapočítává.

Bez tohoto rozšířeného přístupu zůstává zpracování TCO **neúplné** a může vést ke konzervativnímu rozhodnutí setrvat u tradičního on-premise řešení, přestože cloud nabízí **dlouhodobé provozní úspory**, vyšší bezpečnost a strategické výhody.

2.3.2 Riziko neúplné ekonomické analýzy

Rozhodnutí veřejné správy postavená na neúplném TCO vedou k systematickému zkreslení, které upřednostňuje on-premise řešení a podceňuje výhody cloudu. Níže jsou klíčové způsoby, jak se toto zkreslení projevuje, a proč je nutné TCO rozšířit, pokud je to vůbec možné:

1. **Podcenění škálovatelnosti** - standardní TCO obvykle nebere v úvahu, že cloud umožňuje okamžité navyšování či snižování kapacit bez kapitálových investic. Veřejné úřady, které preferují on-premise, často investují do nadměrné kapacity „pro jistotu“, která pak zůstává nevyužitá. Cloudová škálovatelnost ale znamená, že platíte jen za skutečně využitou infrastrukturu a nevznikají náklady na nevyužitou kapacitu.
2. **Ignorování inovačního potenciálu** - tradiční TCO neoceňuje hodnotu rychlejšího vývoje a nasazení nových digitálních služeb. Cloud-native služby (serverless, kontejnerizace, managed AI/ML) umožňují experimentovat a zavádět inovace v řádu dnů místo měsíců, což vede k lepší kvalitě služeb pro občany a úsporám spojeným s lepšími procesy.
3. **Podcenění bezpečnostních přínosů** - ačkoliv se cloud někdy vnímá jako rizikový vůči ochraně dat, velcí poskytovatelé investují do nejmodernějších bezpečnostních technologií: end-to-end šifrování, AI detekce hrozeb, automatizované záplaty a nepřetržitý monitoring. TCO, které tyto externí investice nepočítá, nevystihuje skutečnou úroveň ochrany, kterou cloud přináší, zvláště pro menší úřady bez vlastních SOC týmů.
4. **Přeceňování výhod setrvání u on-premise** - analýza, která vynechává rostoucí náklady na údržbu zastaralých serverů, na energii a licenční poplatky, nadhodnocuje finanční atraktivitu on-premise. Navíc nebere v potaz náklady vyplývající z nutnosti řešit hardwarové havárie, obnovu po neplánovaných výpadcích či zajištění compliance se stále přísnějšími regulacemi.

5. **Opomíjení nákladů kybernetických incidentů** - TCO obvykle nezahrnuje potenciální náklady na odstraňování škod po úniku dat, na právní spory či na reputační ztrátu. Cloudové platformy poskytují integrované nástroje pro detekci, prevenci i zotavení z incidentů, které významně snižují rozsah a dopady útoků.
6. **Nedostatečné zachycení strategické hodnoty** - cloud umožňuje rychle reagovat na nové legislativní požadavky, zdravotní krize či neočekávané špičky v poptávce po e-službách. TCO bez ohledu na tuto pružnost nevystihuje hodnotu kontinuity služeb a schopnosti rychle rozšířit kapacitu podle aktuálních potřeb.

Pouze komplexní TCO, které:

- zahrne migrační náklady (dual-run, refaktoring aplikací, školení)
- zváží compliance a recertifikační poplatky
- ocení bezpečnostní přínosy a minimalizovaná rizika incidentů
- zohlední hodnotu agility, inovací a spokojenosti uživatelů
- promítne environmentální dopady a „cost of trust“

může poskytnout reálný základ pro rozhodnutí o IT infrastruktuře veřejné správy. **Bez takového rozšíření zůstává TCO nevypovídající metrikou a vede k suboptimálním investicím, které brzdí modernizaci, omezují inovační potenciál a zvyšují dlouhodobé provozní náklady.**

2.3.3 Dlouhodobé dopady nesprávného posouzení nákladů na modernizaci IT ve veřejné správě

Nedostatečná či zkreslená analýza celkových nákladů vlastnictví (TCO) při rozhodování o modernizaci informačních systémů veřejné správy může vést k řadě závažných dlouhodobých negativních důsledků:

1. **Podcenění skutečných nákladů a rozpočtové propady** - pokud TCO nezahrne všechny výdaje, instituce riskují, že se během projektu vyskytnou nepředvídané náklady ve výši desítek procent nad rámec původního rozpočtu. To vede k nutnosti dalších dotačních injekcí, přesunu zdrojů z jiných projektů nebo k rozpočtovým škrtům v klíčových veřejných službách.
2. **Prodloužení harmonogramů a odklad inovací** - neúplné vyčíslení finančních i personálních potřeb migrace často způsobí, že projekty nabírají skluz měsíce až roky. Časová prodleva zpomaluje zavádění nových digitálních služeb, brzdí reakci na legislativní změny a oddaluje přínosy automatizace či škálovatelné infrastruktury.
3. **Ztráta důvěry veřejnosti a politické důsledky** - opakované překročení rozpočtu nebo selhání při dodání projektů oslabuje důvěru občanů v digitální vládu. Ztráta reputace může vést k politickým tlakům, odvolávání klíčových manažerů nebo dokonce ke zrušení i jinak perspektivních modernizačních iniciativ.
4. **Vyšší riziko kybernetických incidentů** - když se na úrovni rozpočtu „šetří“ na bezpečnostních opatřeních a auditech, vznikají zranitelné body v infrastruktuře. Nedostatečné investice do pravidelných aktualizací, penetračních testů nebo záložních mechanismů zvyšují pravděpodobnost výpadků či úniků citlivých dat.
5. **Vendor lock-in a omezená flexibilita** - při neadekvátním otestování nákladů na „exit strategy“ a migraci k jinému poskytovateli může dojít k situaci, kdy veřejná instituce zůstane finančně či technicky vázána na jednoho dodavatele. To omezuje možnost reagovat na inovace na trhu nebo vyjednat lepší podmínky.
6. **Nadměrné provozní náklady na zastaralé technologie** - když modernizace ztratí prioritní financování kvůli nečekaným nákladovým výkyvům, stará on-premise infrastruktura zůstává

v provozu déle, než je bezpečné či efektivní. Rostou tak výdaje na údržbu, energii a podporu agendových systémů, které by mohly být eliminovány cloudovou transformací.

7. **Omezené inovační kapacity a ztráta konkurenční výhody** - veřejné instituce, které nedokážou nasadit agilní a škálovatelné cloudové služby včas, ztrácejí schopnost rychle reagovat na krizové situace (např. pandemie), zavádět nové e-služby či využívat pokročilé technologie jako umělou inteligenci. To vede k postupnému odklonu občanů ke komerčním či alternativním kanálům.
8. **Environmentální dopady** - dlouhodobé provozování neefektivních, lokálních datacenter znamená vyšší spotřebu energie a větší uhlíkovou stopu ve srovnání s optimalizovanými cloudovými regiony. Chybějící investice do moderních, „zelených“ datových center tak negativně ovlivňují udržitelnost veřejné správy.
9. **Zvýšená složitost řízení** - když modernizační projekty selhávají rozpočtově i termínově, vzniká chaos v řízení změn, často s opakovanými revizemi metodik, legislativními odklady a zbytečnými audity. To situaci dále komplikuje a zvyšuje administrativní náklady.

Shrnutí - pouze **komplexní TCO**, které zahrnuje nejen přímé investice a provozní náklady, ale také skryté migrační výdaje, compliance položky, bezpečnostní audity, „cost of trust“, hodnotu agility a environmentální externality, může zajistit, že veřejná správa učiní informované a udržitelné rozhodnutí. Neúplné posouzení nákladů pak vede k řetězci dlouhodobých problémů: od překročení rozpočtů, přes ztrátu důvěry až po omezení inovačních a udržitelných iniciativ.

2.3.4 Většina veřejných institucí není schopna připravit komplexní TCO

Většina veřejných institucí skutečně čelí značným překážkám při přípravě skutečně komplexního TCO, a to z následujících důvodů:

1. **Omezené interní kapacity a znalosti** - veřejné úřady často nemají dostatek specializovaných finančních i technických expertů, kteří by dokázali zmapovat veškeré nákladové položky – od poplatků za datový přenos, přes úpravy existujícího zdrojového kódu (refaktoring aplikací) až po environmentální externality či hodnotu agility. Bez interního týmu schopného provádět detailní hodnocení připravenosti přechodu na cloud a vyčíslit nehmotné přínosy (např. společenské či reputační přínosy) selhává úplnost analýzy.
2. **Rozložení odpovědností a řízení** - zodpovědnost za IT rozpočet, bezpečnost, právní compliance a strategii cloudové transformace bývá rozptýlena mezi různá oddělení (IT, finance, právní, bezpečnostní kancelář), která často pracují podle odlišných metodik a mají nesjednocené nástroje. Chybí centrální „owner“ TCO procesu – ekvivalent britského Government Digital Service nebo italského DTD, a tím i koordinace rozsáhlých datových sběrů a kalkulací.
3. **Nedostatek jednotných nástrojů a standardů** - bez národně definovaných postupů, instituce nemají jasný vzor, jakým způsobem zacházet s migračními náklady, compliance výdaji nebo auditními cykly. Když chybí standardizovaný TCO framework, každá organizace si vyvíjí vlastní přístup, což vede k neporovnatelným a často neúplným výsledkům.
4. **Skryté a nefinanční položky zůstávají mimo kontrolu** - klíčové složky jako „cost of trust“ (krize reputace), environmentální externality či business agility value (schopnost organizace rychle reagovat na nové požadavky) se obtížně kvantifikují a běžné účetní nástroje je nezachytí. Instituce tak často vycházejí z podceněných CAPEX/OPEX odhadů, ale opomíjejí významné položky, které později vedou k rozpočtovým výkyvům.
5. **Tlak na rychlé schválení a krátkodobé rozpočty** - veřejné rozpočtové cykly bývají krátké (1–2 roky), zatímco komplexní TCO vyžaduje pětileté až desetileté horizonty.

6. **Psychologie „setrvání u známého“** - když chybí kompletní TCO obraz, je pro úředníky jednodušší argumentovat pokračováním provozu stávajících on-premise systémů než čelit nejistotě nových položek v neznámém modelu. To podporuje konzervativní rozhodnutí, která mohou v dlouhodobém horizontu vést k vyšším provozním nákladům a ztrátě konkurenční výhody.

2.3.5 Shrnutí

Ekonomické hodnocení cloud vs. on-premise řešení ve veřejné správě nelze zjednodušit na univerzální doporučení a bohužel ani na tradiční TCO kalkulátor. Zkušenosti analyzovaných zemí ukazují různé úspěšné přístupy.

Zdá se, že inteligentní multi-cloud strategie představují odpověď na **proměnlivé požadavky** moderní veřejné správy, neboť umožňují pružně volit mezi veřejným cloudem, suverénní infrastrukturou a vlastním on-premise provozem tak, aby každá agendová oblast běžela v optimálním prostředí.

Veřejný cloud je vhodný tam, kde je potřeba rychle reagovat na změny zatížení či nasazovat nové digitální služby bez velkých počátečních investic. Obce, úřady či oddělení s omezeným IT týmem mohou v cloudu automatizovat zálohování, aktualizace a monitoring, škálovat podle skutečné zátěže a platit jen za reálně využité prostředky.

Naopak kriticky důležité registry, citlivé personální či finanční systémy a agendy vyžadující plnou kontrolu nad daty a procesy zůstávají nejlépe na **on-premise infrastruktuře** nebo **ve státním cloudu**. Zde je možné zajistit vyšší možnost kontroly vlastních zaměstnanců bezpečnostními prověrkami, přímou odpovědnost za implementaci bezpečnostních opatření; větší možnosti odmítnutí požadavků na vydání zákaznických dat ze zemí mimo EU; schopnost nabídnout SLA na vyšší garantovanou dostupnost než 99,9%, která je obvyklá u komerčních CSP (kteří obvykle nemají smluvní prostor k vyšším SLA).

Hybridní modely, které kombinují veřejný cloud a on-premise/suverénní prostředí, se stávají standardem v celé Evropě. Umožňují provozovat nejcitlivější agendy v bezpečném státním cloudu či vlastních datových centrech a paralelně nasazovat méně kritické aplikace a analytické nástroje v komerčních cloudech. Tím veřejná správa dosahuje souladu s platnou legislativou a bezpečnostními pravidly, aniž by obětovala agilitu, inovace či finanční efektivitu.

Ekonomicky přináší cloud nízké vstupní náklady a flexibilní OPEX model, který eliminuje náklady na nevyužitý hardware, zatímco on-premise investice do vlastních serverů mohou být výhodnější při dlouhodobém stabilním provozu s předvídatelnou zátěží a přísnými SLA. Kombinace obou přístupů podle charakteru agend a předpokládané zátěže umožňuje maximalizovat úspory, zkrátit time-to-market nových služeb i udržet nejvyšší úroveň bezpečnosti a kontroly nad kritickými daty.

Rozhodování mezi cloudem, on-premise a hybridním modelem bez spolehlivého TCO

Tradiční kalkulace celkových nákladů vlastnictví (TCO) často v prostředí veřejné správy selhává, protože úřady nemají dostatek dat o skrytých nákladech (např. bezpečnost, údržba) nebo kvalitativních přínosech (např. flexibilita, rychlost) – viz výše. Pokud TCO nelze spolehlivě sestavit, je vhodné přejít na **vícekriteriální rozhodovací rámec**, který zohledňuje nejen finance, ale i strategické, provozní, bezpečnostní a organizační aspekty. **Tento přístup je inspirovaný evropskými zkušenostmi (např. z Německa a Francie) a umožňuje komplexní hodnocení bez závislosti na neúplných nákladových datech.**

Proč vícekriteriální rámec?

- **Překonává limity TCO**: Zaměřuje se na širší přínosy, jako je rychlost nasazení nových služeb nebo snížení rizik, které TCO obtížně kvantifikuje.

- **Flexibilní aplikace**: Lze ho přizpůsobit velikosti úřadu, typu agendy (např. citlivá data vs. veřejné portály) a dostupným zdrojům.
- **Podpora rozhodování**: Každý faktor se hodnotí bodově (např. 1–5) nebo kvalitativně, což vede k vyváženému skóre pro cloud, on-premise nebo hybrid.

Klíčové faktory pro hodnocení

Možný rámec pro rozhodování o vhodném prostředí pro jednotlivé agendy veřejné správy: každému faktoru přiřaďte skóre v rozmezí 1–5 dle vybrané metodiky (např. matice kritických výběrových kritérií), následně porovnejte varianty řešení (on-premise, cloud, hybrid), preferujte variantu s nejvyšším agregovaným skóre.

Kategorie faktorů:

1. Strategické faktory (dlouhodobá perspektiva a soulad s politikou státu)

- Podpora vládní strategie cloud-first: Ověřte, zda je zvolené řešení kompatibilní s vládní strategií podpory státního/veřejného cloudu a digitalizace služeb veřejné správy, resp. zda je možné daný IS migrovat na služby zapsané v katalogu cloud computingu podle zjištěné bezpečnostní úrovně (BÚ).
- Kompatibilita s informační koncepcí úřadu: ověřte, zda je zvolené řešení v souladu s dlouhodobou koncepcí směřování úřadu.
- Přínos k modernizaci služeb: Hodnoťte, zda varianta podporuje inovace (např. AI, analytika, kontinuální integrace a nasazování, automatizace), eventuálně zda on-premise řešení nabízí stabilní provoz pro kritické agendové systémy.
- Kompatibilita s budoucími trendy: Preferujte taková řešení, která umožňují postupnou, řízenou migraci bez zbytečných rizik (zejména hybridní modely).

Příklad aplikace: Pro veřejné portály s nízkou citlivostí (BÚ 1, 2) je vhodný veřejný cloud. Pro registry s vysokou citlivostí (BÚ 4) preferujte státní cloud nebo on-premise datacentrum, vždy v souladu se zjištěnou bezpečnostní úrovní.

2. Provozní faktory (efektivita, dostupnost, škálovatelnost)

- Automatizace a rychlost nasazení: Cloudové služby umožňují okamžité škálování kapacity a automatizované aktualizace, což snižuje počet výpadků a zvyšuje dosažitelnost (SLA typicky 99,95% a výše).
- Spolehlivost systémů: Hybridní modely kombinují elasticitu cloudu s redundancí on-premise infrastruktury. Vysoká geo-redundance je snáze dosažitelná v cloudu, ale náročná na vlastní prostředky při on-premise provozu.
- Efektivita procesů: Cloudové služby ulehčují IT týmům rutinní správu a údržbu, což je výhoda zejména pro organizace s omezenými interními kapacitami.

Příklad aplikace: Pro aplikace s proměnlivou zátěží (např. daňová přiznání) je cloud efektivnější. Pro interní stabilní systémy záleží na TCO a aktuální fázi životního cyklu HW.

3. Bezpečnostní faktory (kontrola rizik, compliance, ochrana dat)

- Úroveň ochrany a reakce na hrozby: Cloudoví poskytovatelé nabízejí vestavěné bezpečnostní mechanismy (SIEM, DDoS ochrana, automatizovaná detekce incidentů), on-premise řešení poskytují plnou kontrolu nad bezpečnostním rámcem, ale vyžadují vlastní investice do zabezpečení.

- Compliance s právními a regulatorními požadavky: Pro každou agendu ověřte soulad s českým právním rámcem (ZoKB, ZKB, vyhl. č. 190/2023 Sb.), zejména zjištěnou bezpečnostní úroveň (BÚ) IS. Pro IS zařazené do BÚ 4 je povinný státní cloud, případně on-premise. Pro nižší BÚ lze vybírat z katalogu cloud computingu podle příslušné BÚ.
- Schopnost reakce a obnovy: Cloudové služby obvykle nabízejí rychlejší obnovu po výpadku (nutná smluvní garance), on-premise řešení závisí na vlastních zdrojích a připravenosti.

Příklad aplikace: Pro informační systémy podléhající ZoKB a zařazené do BÚ 4 musíte volit státní cloud nebo on-premise. Pro veřejné portály typu rejstřík bez autentizace (nízká citlivost, BÚ 1–2) je dostatečný veřejný cloud s příslušnou certifikací podle katalogu cloud computingu.

4. Organizační faktory (lidské a institucionální zdroje, flexibilita)

- Dostupnost IT kompetencí: Cloud snižuje potřebu specializovaného IT personálu pro správu infrastruktury; on-premise vyžaduje plnohodnotný tým.
- Závislost na dodavatelích: Hybridní a multi-cloud modely snižují riziko uzamčení u jednoho dodavatele (vendor lock-in).
- Flexibilita při změnách: Cloud umožňuje rychlou adaptaci na změny, což je výhoda v dynamickém prostředí veřejné správy.

Příklad aplikace: Malé obce s limitovanými kapacitami profitují z cloudových služeb; velké organizace s vlastními experty mohou volit hybridní modely.

2.4 Bezpečnostní aspekty

Bezpečnostní aspekty IT prostředí ve veřejné správě v Evropě se v posledních letech zásadně proměnily v důsledku rychlého rozvoje cloudových technologií, nových evropských regulací a rostoucích kybernetických hrozeb. Podle statistik ENISA bylo v roce 2024 zaznamenáno více než 11 000 kybernetických incidentů v EU, přičemž veřejná správa představovala 19% všech nahlášených případů[62].Srovnání modelů on-premise, outsourcingu a cloud computingu ukazuje, že právě cloud přináší veřejné správě největší potenciál pro zvýšení bezpečnosti, efektivity i úspor.

Další přehled incidentů je uveden v kapitole 3.6.2 Několik vybraných kybernetických incidentů ve veřejné správě.

On-premise: Tradiční kontrola, ale omezené možnosti

On-premise infrastruktura byla dlouho vnímána jako nejbezpečnější volba díky plné kontrole nad daty a fyzickým prostředím. Veřejné instituce si samy určují bezpečnostní politiky, spravují přístupová práva a zajišťují fyzickou ochranu serverů. Tento model je však náročný na investice do hardwaru, pravidelné aktualizace, školení personálu a průběžné audity. V praxi často dochází k podcenění některých bezpečnostních opatření – zejména v důsledku otevření on-premise systémů pro vzdálený přístup uživatelů přes Internet, což může vést k vyšší zranitelnosti vůči útokům nebo lidským chybám. Nedostatkem je i obtížná škálovatelnost a pomalá reakce na nové hrozby, protože změny vyžadují zásahy do infrastruktury a dlouhé schvalovací procesy[63].

Cloud computing: Moderní bezpečnost a efektivita

Cloud computing představuje v evropské veřejné správě stále častější volbu právě díky svým bezpečnostním a provozním výhodám. Moderní cloudová řešení, zvláště ta certifikovaná podle pokročilých národních standardů (např. BSI C5, SecNumCloud, španělská ENS Security scheme), nabízejí:

- **Pokročilé bezpečnostní technologie** - cloudoví poskytovatelé investují do šifrování, vícefaktorové autentizace, detekce hrozeb pomocí AI a automatizovaných aktualizací bez narušení běžného provozu, které si většina veřejných institucí nemůže dovolit samostatně provozovat[64]
- **Rychlou reakci na nové hrozby** - aktualizace bezpečnostních opatření probíhají centrálně a okamžitě, což minimalizuje okno zranitelnosti oproti on-premise řešením.
- **Škálovatelnost a odolnost** - cloud umožňuje pružné navyšování kapacit i geografickou redundanci, což zvyšuje dostupnost služeb i v případě útoku či havárie[65].
- **Lepší auditovatelnost a compliance** - cloudové platformy nabízí detailní logování, reporting a podporu pro splnění evropských regulací (GDPR, NIS 2), včetně možnosti lokalizace dat v rámci EU a oddělení provozu (sovereign cloud)[66].
- **Efektivitu a úspory** - přechod na cloud umožňuje snížit provozní náklady, eliminovat nevyužitou kapacitu a přesunout investice z kapitálových výdajů na flexibilní provozní model. Studie ECIPE

[62] https://www.consilium.europa.eu/en/policies/top-cyber-threats/

[63] https://lucysecurity.com/on-premise-vs-cloud-choosing-a-security-platform/

[64] https://www.deloitte.com/us/en/insights/topics/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html

[65] https://www.ospi.es/export/sites/ospi/documents/documentos/ENISA_Security-Framework-for-Governmental-Clouds.pdf

[66] https://www.amchameu.eu/system/files/position_papers/eu_guidelines_public_procurement_cloud_services_final.pdf

odhaduje, že modernizace veřejných služeb pomocí cloudu může v EU přinést stovky miliard eur ročně v úsporách a zvýšení produktivity[67].

Bezpečnostní standardy a evropský rámec

Evropské politiky kladou na cloudová řešení vysoké nároky. Certifikace jako německá BSI C5, francouzská SecNumCloud nebo španělská ENS Security scheme vyžadují:

- šifrování dat v klidu i při přenosu,
- řízení přístupových práv a pravidelné audity,
- transparentnost provozu (přístupy k logům) a možnost exportu dat k jinému poskytovateli
- pravidelné penetrační testy a krizové plány.
- transparentnost ohledně fyzického umístění a zpracování dat

Cloudové služby tak nejen splňují, ale často překonávají bezpečnostní úroveň běžných on-premise nebo outsourcovaných řešení, zejména díky sdíleným investicím do nejmodernějších technologií a centralizovanému řízení bezpečnosti.

Shrnutí

Z hlediska bezpečnosti i efektivity provozu je cloud computing v evropské veřejné správě výhodnější volbou než tradiční on-premise. Nabízí vyšší úroveň ochrany dat, rychlejší reakci na hrozby, lepší škálovatelnost i transparentnost a zároveň umožňuje výrazné úspory. Klíčem k úspěchu je ovšem výběr certifikovaných cloudových služeb, důsledné řízení rizik a respektování evropských regulací a standardů. Cloud tak představuje nejen technologickou, ale i strategickou cestu k bezpečnější a modernější veřejné správě v Evropě.

[67] https://ecipe.org/publications/boosting-efficiency-and-quality-in-eu-public-services-egovernment/

2.5 Ekonomické hodnocení různých forem provozu v České republice

V této kapitole Zpracovatel shrnuje výsledky svého zkoumání ve veřejné správě v České republice. Dle zadání budou poznatky rozděleny do tří skupin dle typu subjektů:

- ISVS ústředních orgánů státní správy, které využívají komerční cloud computing, resp. to zvažují (subjekty ve fázi zvažování byly doplněny nad rámec původního zadání po dohodě ze Zadavatelem).
- ISVS využívající produkty od Gordic spol. s r.o. – malé obce,
- ISVS obcí využívajících informační systém KEO4 od A L I S spol. s r.o. – malé obce.

2.5.1 Situace u ústředních orgánů státní správy

Ačkoliv Zpracovatel oslovil řadu ústředních orgánů státní správy, které provozují některý ze systémů v rámci cloud computingu nebo tento provoz zvažují, ani jeden ze zástupců nepředal nákladové rozpočty původních prostředí (on-premise) ve srovnání s cloudovým prostředím.

Často uvádějí důvody, že původní systém není srovnatelný s novým, nový obsahuje upgrade funkčností, změnu vnitřní architektury (např. je centralizovaný oproti decentralizovanému apod.).

Další důvody nepředání finančních podkladů spočívá **v neschopnosti** poskytnout relevantní data pro **TCO kalkulačku** z důvodů roztříštěnosti informací o nákladech v různých částech úřadu. Jedna věc je nákup IT komponent, druhá věc je rozpočet nákladů za prostory, za energie či lidské zdroje. Další problematikou je podceněná bezpečnost. Tyto problémy často vedou k nesprávnému vyhodnocení ekonomické výhodnosti cloudových řešení a k setrvání u zastaralých on-premise infrastruktur.

Následující body mají ambici shrnout hlavní obtíže při sestavování TCO kalkulací. Tyto obtíže se týkají nejen situace u ústředních orgánů státní správy, ale i nižších stupňů. Dopad u ústředních orgánů je samozřejmě větší kvůli rozsahu působnosti, objemu IT systémů či personální situaci. Následující pasáže vyplynuly z diskusí s oslovenými zástupci zejména ústředních orgánů veřejné správy, popř. jejich dodavatelů.

1. Neúplné zachycení bezpečnostních nákladů v on-premise provozu

Problém skrytých bezpečnostních nákladů

Stávající on-premise provoz často ve výpočtu nezahrnuje všechna bezpečnostní opatření, která jsou standardně součástí cloudových služeb. Při porovnávání nákladů tak vzniká zkreslený obraz, kdy se cloud jeví jako dražší řešení[68][69].

Typické chybějící nákladové položky ve výpočtech on-premise TCO:

- Profesionální bezpečnostní monitoring (SOC služby)
- Pravidelné bezpečnostní audity a penetrační testy
- Implementace pokročilých bezpečnostních nástrojů (SIEM, DLP)
- Náklady na compliance a certifikace
- Redundantní zálohovací systémy a disaster recovery
- Fyzické zabezpečení datových center

[68] https://archi.gov.cz/_media/dokumenty:metodika_tco_ict_sluzeb_vs.pdf

[69] https://www.cybersecurity.cz/data/eGovCloud.pdf

Dopad na TCO kalkulaci

Cloudoví poskytovatelé zahrnují tyto bezpečnostní služby do svých ceníků, zatímco **on-premise řešení často operují s nižší úrovní zabezpečení**[70]. Výsledkem je, že při správném zachycení všech bezpečnostních nákladů by byl rozdíl mezi cloud a on-premise řešením výrazně menší nebo by se dokonce obrátil ve prospěch cloudu.

2. Rozpor mezi celkovými náklady a provozními úsporami

Vyšší TCO vs. provozní efektivita

Cloud computing může vycházet v rámci kalkulace TCO dražší než stávající on-premise provoz. Nicméně tato kalkulace často nezahrnuje kvalitativní benefity, které cloud přináší:

Provozní úspory a automatizace:

- Snížení počtu rutinních administrátorských úkonů
- Automatické zálohování a aktualizace systémů
- Centralizované monitorování a správa
- Rychlejší nasazování nových služeb
- Eliminace plánovaných výpadků pro údržbu

Problém kvantifikace soft benefitů

Zpracovatelé TCO pro veřejnou správu mají **obtíže s kvantifikací těchto "měkkých" přínosů**. Úspory času IT personálu, zvýšená spolehlivost služeb nebo rychlejší reakce na incidenty, by měly být součástí finančních hodnot v TCO kalkulátoru nákladů, faktem ale je, že se obtížně převádějí na konkrétní částky. A to i třeba z důvodu, že nejsou sledovány náklady spojené s prací interních pracovníků na těchto jednotlivých činnostech a bez konkrétní částky na faktuře se mohou tyto **náklady jevit jako nepodložené odhady.**

3. Rozdílná vnímání rizik při aplikaci přiměřeného zabezpečení

Absence jasných kritérií pro bezpečnostní požadavky

Úřady a samosprávy zařazené do režimu nižších povinností (§ 14 nZKB), které většinou dříve pod ZKB nespadaly, jsou nyní právně povinny zavést a udržovat systém minimální kybernetické bezpečnosti, který zahrnuje jak organizační, tak technická opatření (řízení aktiv, řízení rizik, řízení přístupu a identit, detekci a zaznamenávání událostí, řešení incidentů, síťovou a aplikační bezpečnost, kryptografické mechanismy) přiměřeně povaze a rizikům jejich informačních systémů.

NÚKIB sice vydává podpůrné metodiky, avšak vzhledem k širokému rozsahu možných opatření a omezeným kapacitám mnoha úřadů bez vlastních odborníků na kybernetickou bezpečnost, může dojít k nejistotě na straně správce ISVS, která konkrétní opatření zvolit a jak je efektivně implementovat. To vede k rozdílům v úrovni zabezpečení a zvyšuje zranitelnost vůči kybernetickým útokům.

Problém subjektivního hodnocení rizik

Některé organizace mohou považovat minimální zabezpečení za dostačující, zatímco jiné požadují vyšší úroveň ochrany bez ohledu na náklady.

[70] https://www.epenize.eu/cloudove-reseni-versus-on-premise/

4. Financování CAPEX vs. OPEX

Dostupnost dotací pro hardware vs. cloud služby

Zásadním problémem je rozdílná dostupnost financování pro různé typy IT investic:

Dotace na hardware a implementaci:

- Operační programy EU umožňují financování nákupu IT vybavení[71]
- Jednorázové investice jsou snáze obhajitelné v rozpočtových procesech
- Implementace nových systémů přímo v cloudu či migrace stávajících systémů do cloudu nejsou častým scénářem

Omezení pro cloud služby:

- **Provozní náklady na cloud nejsou způsobilé pro většinu dotačních programů**
- Pravidelné platby za cloud služby zatěžují provozní rozpočty

Dopad na rozhodovací procesy

Tato asymetrie **systematicky zvýhodňuje on-premise řešení** bez ohledu na jejich skutečnou ekonomickou efektivitu. Organizace často volí méně efektivní, ale dotačně podporované řešení.

5. Vendor lock-in

Vendor lock-in představuje jednu z nejkritičtějších, ale často podceňovaných položek v TCO kalkulacích českých orgánů veřejné správy.

Monolitické vs. modulární architektury

Většina informačních systémů českých OVS vznikla v období 90. let a první dekádě 21. století jako monolitické aplikace. Tyto systémy představují zásadní překážku pro přechod do cloudu:

- Těsná provázanost komponent - změna jedné části vyžaduje úpravy v celém systému
- Závislost na specifickém hardware - systémy optimalizované pro konkrétní servery nebo procesory
- Proprietární databázové struktury - využití nestandardních datových formátů
- Absence API - komunikace mezi systémy řešena na úrovni databáze nebo souborů.

Tento stav většinou vyžaduje kompletní přepracování systému na novou architekturu většinou i s novými funkčnostmi. V takovém případě nedochází k prosté migraci, ale současně k budování nového systému, což má na výsledek TCO zásadní vliv, a je to jeden z hlavních argumentů zástupců OVS pro neporovnatelnost kalkulací „předtím a po“.

6. Vliv manažerských ambicí na IT rozhodování

Kontrola nad IT zdroji jako mocenský nástroj

Osobní ambice IT manažerů hrají významnou roli v rozhodování o cloudových vs. on-premise řešeních. Přechod na cloud může být vnímán jako:

Ohrožení manažerské pozice:

- Snížení počtu podřízených IT specialistů
- Ztráta kontroly nad technickou infrastrukturou

[71] https://www.prehleddotaci.cz/operacni-program/digitalni-podnik

- Redukce rozpočtu IT oddělení
- Vyšší závislost na externích poskytovatelích

Organizační odpor vůči změnám

IT manažeři mohou **záměrně nebo na základě nedostatečné informovanosti nadhodnocovat rizika cloudu** nebo podhodnocovat náklady on-premise řešení, aby obhájili zachování stávajícího stavu. Tento jev je umocněn v prostředí veřejné správy, kde je změna vnímána jako riziková a kde chybí tržní tlaky na efektivitu.

7. Obavy ze splnění compliance a reakce na audity

Nově zavedené regulace NÚKIB jako katalyzátor změn

Požadavky NÚKIB na kybernetickou bezpečnost často fungují jako externí tlak nutící organizace k přehodnocení svých IT řešení:

Typické compliance požadavky:

- Implementace bezpečnostních opatření podle vyhlášky č. 82/2018 Sb.
- Pravidelné analýzy rizik a jejich řízení
- Hlášení kybernetických bezpečnostních incidentů
- Vyhodnocování bezpečnostních úrovní pro poptávaný cloud computing

Reaktivní vs. proaktivní přístup

Organizace často **reagují na audity a kontroly až ex post**, kdy jsou nuceny rychle implementovat bezpečnostní opatření. V takových situacích může cloud představovat rychlejší cestu ke compliance než budování vlastní bezpečnostní infrastruktury[72][73].

Problém reaktivního přístupu:

- Nedostatek času na kvalitní TCO analýzu
- Rozhodování pod tlakem regulátorů
- Preference rychlých řešení před ekonomicky optimálními
- Riziko vendor lock-in při uspěchaném výběru

Souhrnně lze říci, že **celková cena vlastnictví (TCO) cloudu** v českém veřejném sektoru je často nadhodnocena, protože staré on-premise prostředí skrývá část nákladů a požadavky na kybernetickou bezpečnost, provozní režii, které nejsou v kalkulacích dopočítány.

2.5.2 Situace v malých obcích

Malé obce, kterých se průzkum týkal, byly obce s počtem obyvatel do 5 000, přičemž obce s produkty od Gordic byly obcemi s počtem obyvatel do 2 000.

2.5.2.1 Obce do 2 000 obyvatel

Situace ve zkoumaných obcích do 2 000 obyvatel vykazovala společné rysy:

- Využívaly většinou produkty společnosti Gordic spol. s r.o. (tato skutečnost zohledňuje pouze vybrané obce, trend na trhu může být jiný)

[72] https://www.businesswatchgroup.co.uk/why-cloud-based-security-is-safer-than-on-premise-in-2025/

[73] https://www.milestonesys.com/resources/content/articles/cloud-based-surveillance-security/

- Ve výchozí situaci „on-premise“ prostředí provozovaly „ploché sítě“ s pár počítači a tiskárnami.
- Zastaralé systémy: některé úřady provozují kvůli omezenému rozpočtu Home edice OS a nekonzistentně aktualizovaný software s nižší úrovní zabezpečení.
- Nedostatečná segmentace počítačové sítě úřadu a absence moderních bezpečnostních nástrojů (firewally, SIEM) zvyšuje riziko vniknutí malwaru či ransomwaru.

Vzhledem k tomu, že většina ze zkoumaných obcí nebyla schopna udat hodnoty / náklady hardwarového řešení použitého v on-premise řešení, Zpracovatel nakonfiguroval potřebný HW včetně odhadu jeho nákladů, a to v souladu se Zadáním studie, které uvádí: „*V případě, že on-premise nebo klasický outsourcing nesplňuje/nesplňoval při předcházející formě provozu všechna kritéria bezpečnosti vyžadovaná pro ISVS dané bezpečnostní úrovně, je do nákladů předcházející formy provozu potřeba připočíst odhad nutných nákladů na zavedení dodatečných bezpečnostních opatření, které vyžaduje příslušná bezpečnostní úroveň“.* Aktuální výše zastaralého a nedostatečného IT prostředí byla také odhadnuta na úrovni informací, které Zpracovatel od obce získal.

Byla přitom uvažována varianta vlastního serveru včetně potřebných licencí, zálohování, ale i předpokládaných nákladů v souvislosti s umístěním prostředí – Housing (náhradní napájení, dodávka elektřiny, fyzické zabezpečení apod.).

Protože výběr obcí pracuje v on-premise provozu zejména s produkty společnosti GORDIC, použili jsme konfiguraci odpovídající daným požadavkům.

MIN a MAX varianta nákladů na IT prostředí

Pro výpočet srovnávacích TCO v jednotlivých obcí budeme uvažovat následující odhad nákladů pro „on-premise“ IT prostředí

MAX Varianta

Defaultní HW pro malé obce obsahuje nutné licence v placené (nikoliv open) verzi. Týká se jednorázových nákladů. Jedná se o maximalistickou verzi kalkulace nákladů na IT infrastrukturu.

Hodnota **jednorázových nákladů** na zabezpečení požadovaného defaultní HW pro malé obce za předpokladu **zakoupení** všech nutných licencí činí **225 000 Kč vč. DPH**.

Hodnota ročních provozních nákladů činí **42 000 Kč vč. DPH**.

Celkové TCO (5 let) tohoto IT prostředí činí 435 000 Kč vč. DPH.

MIN Varianta

Defaultní HW pro malé obce využívá některé open licence nebo licence získá jiným způsobem. Není možné u všech licencí, jen vybraných. Týká se jednorázových nákladů. Jedná se o minimalistickou verzi kalkulaci nákladů na IT infrastrukturu.

Hodnota **jednorázových nákladů** na zabezpečení požadovaného defaultní HW pro malé obce za předpokladu **zakoupení** všech nutných licencí činí **109 800 Kč vč. DPH**.

Hodnota ročních provozních nákladů činí **42 000 Kč vč. DPH**.

Celkové TCO tohoto IT prostředí činí 295 000 Kč vč. DPH.

Poznámky k Variantě MAX i Variantě MIN:

- **Varianta MAX** představuje maximalistickou verzi zajištění legálního IT prostředí se zajištěním veškeré podpory. Celkové náklady maximalistické varianty činí **435 000 Kč vč. DPH.**
- **Varianta MIN** představuje minimalistickou verzi zajištění IT prostředí pomocí open licencí, popř. licencí získaných jiným způsobem, Celkové náklady maximalistické varianty činí **295 000 Kč vč. DPH.**

- Náklady na pořízení vhodného „on-premise“ IT prostředí se tedy pohybují mezi **295 000 - 435 000 Kč bez DPH.** Open licence v minimalistické verzi mohou vyvolávat dodatečné náklady na správu prostředí, kdy tato je u placené verze plně zajištěna. V případě maximalistické verze může obec nalézt rezervy v rámci jiných položek.

TCO (5 let) jednotlivých variant

Na základě výše uvedených kalkulovaných nákladů na IT prostředí jsme hodnotili skutečnou situaci on-premise řešení a přechod na cloud. Srovnání zahrnuje:

- skutečný nedostatečný/zastaralý on-premise provoz, kde byla část nákladů na prostředí provozu Zpracovatelem odhadnuta s ohledem na skutečný stav prostředí v konkrétní obci,
- kalkulovaná MIN a MAX varianta, kde byla část nákladů na prostředí provozu Zpracovatelem odhadnuta v souladu se Zadáním studie *V případě, že on-premise nebo klasický outsourcing nesplňuje/nesplňoval při předcházející formě provozu všechna kritéria bezpečnosti vyžadovaná pro ISVS dané bezpečnostní úrovně, je do nákladů předcházející formy provozu potřeba připočíst odhad nutných nákladů na zavedení dodatečných bezpečnostních opatření, které vyžaduje příslušná bezpečnostní úroveň“,*
- skutečný aktuální provoz v rámci cloud computingu.

Výsledky v obcích se v zásadě shodovaly:

- TCO provozu informačního systému na **zastaralém on-premise IT prostředí** s minimální bezpečností samozřejmě vycházel pro všechny obce **zdánlivě výhodněji** než pořizované cloudové služby (nebo předložené aktuální nabídky).
- Při výpočtu TCO se započtením odhadovaných nákladů na **zabezpečené on-premise IT** prostředí by byly TCO náklady na pořízení tohoto IT prostředí **vyšší v minimální i maximální variantě** nákladů než pořizované cloudové služby (nebo předložené aktuální nabídky).

V případě všech pěti obcí vychází cloudové řešení jako výhodnější varianta provozu. Zdánlivě výhodný zastaralý on-premise provoz je z hlediska bezpečnosti absolutně nevhodný a prakticky neošetřuje jediné riziko. Při započítání odhadu nutných nákladů na zavedení dodatečných bezpečnostních opatření (MAX a MIN) varianta, vychází provoz v on-premise prostředí jako jednoznačně dražší. **Cloudové řešení je u sledovaných obcí v průměru minimálně o 37% levnější.**

2.5.2.2 Obce do 5 000 obyvatel

Situace ve zkoumaných obcích do 5 000 obyvatel byla výrazně odlišná od zkoumaných obcí do 2 000 obyvatel. Obce:

- ve výchozí situaci „on-premise“ prostředí měly poměrně výrazně zainvestováno do serverů, potřebných licencí souvisejících s provozem ISVS, vyřešený housing,
- byly k dispozici vypovídající ekonomické podklady o investicích do on-premise,
- IT prostředí se dalo označit za vyhovující i z hlediska bezpečnosti.

Zpracovatel tak **nemusel odhadovat náklady** pro zabezpečený provoz, ale **mohl přímo** využít údaje poskytnuté obcí. Srovnání tak obsahuje přímé srovnání skutečných nákladů vynaložených na on-premise provoz a nákladů vynakládaných aktuálně v rámci cloud computingu. Průzkumu se zúčastnily pouze 2 obce.

Z pohledu bezpečnosti považují zástupci obou obcí situaci za srovnatelnou. Dle názoru Zpracovatele přece jen převládá výhoda na straně cloudu, a to z důvodu stálého monitoringu prostředí cloudu. Z dotazníků zaměřených na úroveň kybernetické bezpečnosti plyne, že monitoring nebyl ve srovnatelném rozsahu v on-premise prostředí realizován a provozován. Nicméně rizika, která byla popsána v případě menších obcí do 2 000 obyvatel, byla z větší části mitigována. **V případě obou obcí vychází cloudové řešení jako výhodnější varianta provozu.**

2.6 Závěry a shrnutí

Cílem studie bylo odpovědět na otázku: Jaké jsou ekonomické a bezpečnostní rozdíly provozování informačních systémů veřejné správy (dále jen „ISVS“) různými formami?

Studie by rovněž měla přispět k potvrzení nebo vyvrácení hypotézy, že provoz ISVS formou cloud computingu je ekonomicky výhodnější a umožňuje snáze dosažení požadované úrovně bezpečnosti ISVS.

2.6.1 Zahraniční zkušenosti

Zkušenosti z různých evropských zemí ukazují, že migrace na cloudové služby přináší veřejné správě významné úspory nákladů, zvýšení efektivity a zlepšení dostupnosti digitálních služeb. Například ve Švédsku, Dánsku či Estonsku vedla centralizace řízení a sdílení cloudových služeb k efektivnějšímu využívání zdrojů, snížení provozních nákladů a rychlejšímu zavádění nových služeb.

Podobně v Německu a Francii umožňuje cloudová strategie snížit provozní a investiční náklady, lépe sdílet infrastrukturu mezi úřady a posílit vyjednávací pozici vůči dodavatelům. Italský transformační model ukazuje, že centrálně řízená migrace do cloudu může přinést úspory stovek milionů eur ročně jen na provozních nákladech regionálních a místních samospráv. Kromě finančních benefitů přináší cloud také vyšší flexibilitu, škálovatelnost a možnost rychle reagovat na nové požadavky občanů i legislativy.

Výhodnost přechodu na cloud je však podmíněna správným nastavením governance, bezpečnostních standardů a transparentními pravidly pro ochranu dat. Evropské politiky, jako GDPR, NIS 2 nebo Data Act, nastavují vysoké požadavky na bezpečnost a interoperabilitu, což zajišťuje důvěru veřejnosti a ochranu citlivých údajů. Zároveň zkušenosti ukazují, že úspěšná cloudová transformace vyžaduje systematickou podporu migrace, vzdělávání zaměstnanců a centralizované řízení změn. **Zkušenosti ukazují, že v případě některých systémů, resp. dat, není cloud vhodným řešením nebo je nutné posoudit jaký typ cloudu zvolit.**

Celkově lze však uzavřít, že přechod veřejné správy na cloud v evropském kontextu je ekonomicky i provozně výhodný, pokud je realizován v souladu s moderními bezpečnostními a správními standardy a s ohledem na odstupňované požadavky na digitální suverenitu.

2.6.2 Výsledky průzkumu v ČR

1. Ústřední orgány veřejné správy

Nedostatečná datová základna pro analýzu

Ústřední orgány státní správy neposkytly nákladové rozpočty potřebné pro objektivní srovnání původních on-premise prostředí s cloudovými řešeními. Tato absence dat představuje zásadní překážku pro ekonomické hodnocení.

Zástupci těchto úřadů argumentují, že původní systémy nejsou srovnatelné s novými díky upgradům funkcionalit a změnám vnitřní architektury.

Další problém spočívá v neschopnosti sestavit TCO kalkulačku z důvodu roztříštěnosti informací o nákladech napříč různými částmi úřadu. Systémové problémy TCO kalkulací dle provedených rozhovorů se zástupci ústředních orgánů či jejich dodavatelů zahrnují:

- neúplné zachycení bezpečnostních nákladů,
- provozní efektivita vs. celkové náklady,
- rozdílná vnímání rizik při aplikaci přiměřeného zabezpečení)

Souvisejícím argumentem jsou strukturální překážky přechodu na cloud:

- financování CAPEX-OPEX
- vendor lock-in a monolitické agendové systémy
- manažerské faktory
- obavy ze splnění požadavků v oblasti Compliance

V případě zkoumání u ústředních orgánů veřejné správy ČR tedy nelze kvůli nedostatku informací jednoznačně potvrdit ekonomickou výhodnost přechodu na cloudový provoz. Při rozhodování o přechodu na cloud nebo setrvání v on-premise prostředí bude nutné zvážit i další aspekty s ohledem zejména na kritičnost systému a citlivost dat (viz vícekriteriální rozhodování, kapitola 2.3.5 Shrnutí). Neschopnost zástupců této veřejné správy sestavit TCO kalkulace sama ukazuje na složitost celkového problému.

2. Malé obce

Obce do 2 000 obyvatel

Analyzované obce do 2 000 obyvatel vykazovaly společné charakteristiky. Ve výchozí situaci provozovaly "ploché sítě" s několika počítači a tiskárnami, zastaralé systémy s nižší úrovní zabezpečení. Nedostatečná segmentace sítě a absence moderních bezpečnostních nástrojů zvyšovala riziko vniknutí malwaru či ransomwaru.

Ekonomické vyhodnocení - Zpracovatel nakonfiguroval potřebný hardware včetně odhadu nákladů v souladu se zadáním studie. Byl uvažován vlastní server s potřebnými licencemi, zálohováním a náklady na housing. Pro výpočet TCO byly stanoveny dvě varianty:

- MIN varianta: Defaultní hardware s využitím některých open licencí nebo licencí získaných jiným způsobem. Jednorázové náklady činily 109 800 Kč vč. DPH, roční provozní náklady 42 000 Kč, celkové TCO (5 let) 295 000 Kč vč. DPH.
- MAX varianta: Maximalistická verze s nákupem všech nutných licencí v placené verzi. Jednorázové náklady činily 225 000 Kč vč. DPH, roční provozní náklady 42 000 Kč, celkové TCO (5 let) 435 000 Kč vč. DPH.

Ve všech pěti obcích vychází cloudové řešení jako výhodnější varianta provozu. Zdánlivě výhodný zastaralý on-premise provoz je z hlediska bezpečnosti absolutně nevhodný. Při započítání odhadu nutných nákladů na zavedení dodatečných bezpečnostních opatření vychází provoz v on-premise prostředí jako jednoznačně dražší.

3. Obce do 5 000 obyvatel

Situace ve zkoumaných obcích do 5 000 obyvatel byla výrazně odlišná. Tyto obce měly ve výchozí situaci značně zainvestováno do serverů, potřebných licencí souvisejících s provozem ISVS a vyřešený housing. IT prostředí se dalo označit za vyhovující i z hlediska bezpečnosti.

Ekonomické vyhodnocení - Zpracovatel mohl přímo využít údaje poskytnuté obcí pro srovnání skutečných nákladů vynaložených na on-premise provoz s náklady na cloud computing. Z pohledu bezpečnosti považují zástupci obou obcí situaci za srovnatelnou, přičemž převládá výhoda na straně cloudu z důvodu stálého monitoringu prostředí. K dalším výhodám může patřit zajištění služeb 24x7 či bezpečné přihlašování do systému z míst mimo úřad. V případě obou obcí vychází cloudové řešení jako výhodnější varianta provozu.

Závěrečné shrnutí

Cloud computing představuje optimální řešení pro orgány veřejné správy, protože:

1. **Ekonomicky** - TCO je pro provoz IS v cloudu při správném výpočtu (tj. zahrnutí všech relevantních složek) a zajištění srovnatelné úrovně bezpečnosti nižší než u zabezpečeného on-premise provozu
2. **Bezpečnostně** - poskytuje vyšší úroveň ochrany než většina stávajících on-premise řešení
3. **Provozně** - snižuje administrativní zátěž a zvyšuje spolehlivost
4. **Strategicky** - umožňuje rychlejší digitalizaci a modernizaci veřejné správy

Na základě výše uvedeného lze doporučit systematický přechod na cloud computing s prioritou pro malé obce, které z něj budou mít největší přínos, a postupnou migraci ústředních orgánů s ohledem na specifika jejich agendových systémů.

2.6.3 TCO model ve veřejné správě

Následující pasáže vyplynuly z diskusí s oslovenými zástupci zejména ústředních orgánů veřejné správy, popř. jejich dodavatelů.

Současná praxe používání TCO (Total Cost of Ownership) kalkulačky v českých orgánech veřejné správy při rozhodování o přechodu na cloud computing **naráží na řadu problémů při vyplňování.**

Za prvé, zpracovatelé **podhodnocují náklady stávajícího on-premise provozu**, protože opomíjí výdaje na bezpečnostní monitoring prostřednictvím SOC, pravidelné audity a penetrační testy, pokročilé nástroje typu SIEM a DLP, splnění compliance a certifikačních požadavků, redundantní zálohování, disaster recovery i fyzické zabezpečení datových center. Zároveň nejsou schopni vyčíslit kvalitativní přínosy cloudu, jako je automatizace rutinních úkonů, snížení výpadků, rychlejší nasazování nových funkcionalit, centralizované řízení či eliminace plánovaných odstávek.

Druhým problémem jsou **nedostatky rozhodovacího procesu a vnímání rizik na straně zpracovatele**. Situaci komplikuje i konflikt zájmů IT manažerů, kteří mohou preferovat setrvání u on-premise, aby si udrželi počet podřízených, kontrolu nad infrastrukturou a rozpočtem a nižší závislost na externích dodavatelích.

Třetí oblast představuje **systémové zkreslení vnímání financování**. Dotační politika dlouhodobě zvýhodňuje kapitálové výdaje na hardware, protože jsou způsobilé pro evropské fondy, zatímco průběžné platby za cloudové služby většinou nikoli. Úřady proto snadněji obhájí jednorázovou investici z dotačních prostředků než pravidelné provozní platby, což vede k nerespektování výsledků TCO kalkulace: rozhodování pak neodráží skutečnou ekonomickou efektivitu, ale primárně možnost uplatnění dotací. Z dotací (CAPEX) by sice mohlo být financováno i budování nových systémů přímo v cloudu nebo migrace do cloudů, nicméně tyto scénáře nejsou časté. TCO opomíjí časovou hodnotu peněz a souvislost s časově vymezenou dostupností investičních zdrojů veřejné správy.

Čtvrtým nedostatkem může být převážně reaktivní, nikoli strategický charakter rozhodování. Úřady občas **implementují bezpečnostní opatření** až po kontrolách NÚKIB, takže se pod tlakem regulátorů rozhodují rychle a nikoli podle důkladné analýzy. TCO v takových situacích nemůže sloužit jako relevantní podklad, protože chybí čas na jeho kvalitní zpracování.

Shrnutí: Doplnění TCO kvalitativním hodnocením

Alternativní rozhodovací rámec pro přechod na cloud může doplnit tradiční TCO kalkulačku vícekriteriálním hodnocením, které zohledňuje **strategické, provozní, bezpečnostní a organizační faktory**.

Strategické faktory zahrnují především soulad s vládní strategií podpory cloudu[74], tedy zvážení cloudových řešení před vlastním on-premise provozem či míru, v níž nová služba z hlediska možné modernizace využitím cloudových služeb přispěje k digitalizaci veřejné správy.

Provozní faktory se zaměřují na schopnost cloudu automatizovat a efektivně řídit rutinní procesy, na rychlost nasazení nových funkcionalit a na zajištění vysoké spolehlivosti a dostupnosti poskytovaných služeb.

Bezpečnostní faktory vyhodnocují současnou úroveň ochrany dat a aplikací, soulad s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), a dále schopnost poskytovatele implementovat v cloudu bezpečnostní opatření, která by on-premise byla nepřiměřeně nákladná nebo úplně nemožná, a dále schopnost reagovat na zjištěné hrozby i hlásit a zvládat incidenty v předem definovaných lhůtách.

Organizační faktory kladou důraz na dostupnost interních kompetencí v oblastech IT a informační bezpečnosti, aby organizace nebyla nadměrně závislá na externích dodavatelích, a na flexibilitu při přizpůsobování služeb měnícím se požadavkům.

Tento vícekriteriální přístup umožňuje komplexně porovnat on-premise a cloudová řešení nejen z hlediska nákladů, ale i z pohledu strategického směřování, provozní efektivity, bezpečnostní zralosti a organizační připravenosti.

Stávající využití TCO kalkulačky tak může v konečných důsledcích poskytovat neúplné výsledky, které mohou zkreslit rozhodování ve prospěch on-premise řešení. Doplnění TCO o vícekriteriální hodnocení by umožnilo: objektivnější hodnocení všech aspektů cloudových řešení, eliminaci konfliktu zájmů IT manažerů, strategické rozhodování v souladu s vládními prioritami a rychlejší modernizaci veřejné správy.

[74] https://archi.gov.cz/uvod_klicove_oblasti#cloud

3. DETAILNÍ INFORMACE

Následující kapitoly rozvádějí do detailů a zpřesňují klíčové nálezy identifikované v předchozí kapitole.

3.1 „SEVERNÍ MODEL“

Tabulka 2 – „Severní model“ – charakteristika postupů Švédska, Dánska a Estonska při provozu ISVS

Kritérium	Švédsko	Dánsko	Estonsko
Centrální politika	Cloud-first od roku 2022 (vládní rámec „Cloud Clarity“).	Digitaliserings-strategi 2024 – 2027 + „Offentligt Cloudprincip“ (vládní privátní cloud + certifikovaný public cloud).	Digital Agenda 2018–2030: „Once-only + Cloud by default“.
Národní/Gov cloud	SIGO GovCloud (spravuje Statens Servicecenter) pro ústřední úřady; provoz na dvou švédských DC, ISO 27001/C5.	Statens IT-Cloud pro ministerstva; KOMBIT Shared Cloud pro 98 municipalit; regionální zdravotnictví běží v hybridu.	Riigi Pilv („Government Cloud“) + X-tee (X-Road) jako státní datová páteř.
Klíčové prvky pro kraje / obce	- Program SKR KommSynCloud – balík SaaS pro všechny obce (ERP, HR, GIS). - „Handshake for Digitalisation“ = centrální investiční fond (1 mld. SEK/rok).	- KOMBIT nakupuje a provozuje společné aplikace (Úložiště spisů, Dánský adresní registr apod.). - Obce platí pouze variabilní OPEX/obyvatele.	- Všechny obce napojeny na X-Road a využívají SaaS v Riigi Pilv. - Stát provozuje Riigi Infosüsteemi Amet (RIA) pro 24/7 SOC a backup site v Tartu.
Standardy a bezpečnost	- Profil „SWE GOVSEC“ – kombinace ISO 27001 + švédská OSA-klassning. - Data mimo SEK vyžadují šifrování s HSM ve Švédsku.	- Profil ISO 27001 + ISO 27701; všechny cloudové kontrakty musí projít Danish Risk Model. - Data EU-only, výjimky schvaluje Datatilsynet.	- Bezpečnostní třídy ML1–ML4; ML4 jen v Riigi Pilv. - eID + e-Signature povinné pro všechny transakce; Zero-Trust architektura státu.
Financování a governance	- SKR (svaz obcí) vyjednává rámcové dohody – úspora ≈ 28% nákladů.	- Centralizované financování z „Digital Leap“ fondu (5 mld. DKK 2022-25).	- Unified budget: 1% z každého ministerstva jde do Digital Innovation Fund; RoI 6:1.
Výsledek 2024	- > 70% centrálních IS v SIGO, regiony 60% hybrid. - 98% obcí užívá alespoň 3 služby KommSynCloud.	- Vládní úřady: 80% workloadů v Statens IT-Cloud. - Municipality: 85% SaaS v KOMBIT, zbytek specializované legacy.	> 99% veřejných e-služeb běží v Riigi Pilv/X-Road. - Výpadek kritických systémů < 5 min/rok.

Společné rysy „severního“ přístupu

„Severní“ přístup ke cloudové transformaci veřejné správy kombinuje **centrálně řízenou infrastrukturu** se **silnou místní autonomií**. Podle tohoto modelu stát provozuje jednu **sdílenou páteř** – národní gov-cloud, která poskytuje služby IaaS a PaaS pro většinu vládních agend, zatímco ministerstva smějí budovat vlastní datová centra pouze pro systémy, zpracovávající utajované informace. Kraje a obce naopak dostávají hotové komerční balíčky SaaS – například moduly pro finanční řízení, agendové systémy či personalistiku – a nemusí se sami starat o nákup hardwaru ani jeho údržbu. V tuto chvíli to

samozřejmě neznamená, že všechny úřady již využívají cloud ke všem svým aktivitám, ale řízeně se směřuje k tomuto cíli.

Klíčem k úsporám jsou **sdílené nákupy**. V Dánsku konsorcium KOMBIT uplatňuje principy sdíleného financování, např. model licencování „na obyvatele obce“, takže i malá obec pod pět tisíc obyvatel platí za konkrétní aplikaci formou služby stejnou jednotkovou cenu za obyvatele jako hlavní město Kodaň. Ve Švédsku svaz obcí SKR vyjednává celostátní rámcové smlouvy s volitelnými moduly, přičemž jednotliví dodavatelé komunikují pouze s jednou centralizovanou autoritou, čímž se zjednodušuje správa a dosahují se výrazné úspory z rozsahu.

Bezpečnost provozu zajišťuje stát prostřednictvím profesionálních SOC center s nepřetržitým auditem. V oblasti státních SOC center, ve Švédsku tuto roli plní Myndigheten för digital förvaltning, v Dánsku Center for Cybersikkerhed a v Estonsku Riigi Infosüsteemi Amet (RIA). Místní úřady se tak mohou plně soustředit na správu svých agend, aniž by musely mít vlastní experty na provoz sítí či bezpečnostní monitoring.

Nezbytným základem fungování tohoto modelu je také široce využívaná digitální identita pro občany a interoperabilita IS veřejné správy. Všechny čtyři země zavedly státem řízené identitní systémy – BankID ve Švédsku, MitID v Dánsku a eID v Estonsku – které pokrývají téměř 100% dospělé populace a umožňují autentizaci a autorizaci uživatelů ve všech veřejných i soukromých digitálních službách.

Všechny státní i obecní služby konzumují centrální API (X-Road, Danish Service Platform, Swe InterConnect).

Odlišnosti tří zemí

Tabulka 3 – Odlišnosti tří zemí

Faktor	Švédsko	Dánsko	Estonsko
Řízení	Federativní – SKR vyjednává za obce, ale provoz DC spravuje stát. Centrální strategie	Trojice: Ministerstvo financí (politika), Digitaliseringsstyrelsen (standardy), KOMBIT (operátor obcí).	Silně centralizované (RIA + Riigi Pilv) s povinným připojením všech veřejných entit na páteřní X-Road.
Technologie	AWS Stockholm + Azure SE + lokální OpenShift v SIGO.	Statens IT = VMware Sovereign Cloud; obce – KOMBIT OpenStack.	Riigi Pilv běží na Nutanix; X-Road je open-source middleware.
Financování cloudu	„Pay-as-you-grow“: odvod 0,35% rozpočtu každého úřadu na centrální služby.	State Cloud: náklady na uživatele / obyvatele obce (DKK 105/rok), obce platí DKK 85/obyvatel.	E-residency poplatky a EU fondy kryjí 35% provozu Riigi Pilv.

Dopady

Externí audity potvrzují, že organizace veřejného sektoru dosahují **20–30% úspory celkových nákladů vlastnictví (TCO) oproti historickým on-premise datovým centrům již po třech letech provozu**[75]. Z hlediska kybernetické bezpečnosti centralizovaný monitoring umožňuje detekovat a reagovat na incidenty ve zlomku původní doby – průměrný čas obnovy služby (MTTR) v Estonsku klesl v roce 2024 na **34 minut**, oproti dřívějším dnům[76]. Co se týče dostupnosti digitálních služeb, Estonsko a Dánsko nabízejí **více než 90% agend online 24/7**, zatímco ve Švédsku je tento podíl 85%.

[75] https://www.cloudzero.com/blog/cloud-computing-statistics/

[76] https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/06/oecd-reviews-of-digital-transformation-going-digital-in-sweden_g1g904ac/9789264302259-en.pdf

Severní vzorec úspěchu: silné politické rozhodnutí, centralizované řízení a sdílené financování vedly k rychlé a masové adopci cloudu napříč všemi stupni veřejné správy při současném zvýšení kybernetické bezpečnosti a snížení TCO.

Klíčové technologie a infrastruktura „Severního modelu“

Tabulka 4 – Klíčové technologie a infrastruktura „Severního modelu“

Vrstva	Švédsko	Dánsko	Estonsko	Společné rysy
Státní/Gov-cloud	SIGO GovCloud (Statens Servicecenter) – dvě zrcadlená DC ve Stockholmu, VMware vSphere + Kubernetes na bare-metal, objektové úložiště MinIO; šifrování dat striktně v HSM FIPS 140-2	Statens IT-Cloud (ústřední orgány) a KOMBIT Shared Cloud (98 obcí) – OpenStack + Ceph v geo-replikovaných DC; API řízené Terraform/Kolla-Ansible	Riigi Pilv – hyperkonvergovaná platforma Nutanix AOS; všechny služby běží jako cloud-native kontejnery řízené OpenShift; záložní uzel v Tartu	– Výhradně evropská lokalita dat – Identické SLA pro IaaS/PaaS (99,95%) – Povinné certifikace ISO 27001 / 27701 + národní profily
Identita a přístup	Swedish Interconnect API Gateway (WS-Security + REST)	**Danish Service Platform** (SOAP/REST, GraphQL) + NemLog-in broker	**X-Road (X-tee)** – decentralizovaná mTLS výměna dat	– „Once-only“ princip; všechny úřady musí poskytovat otevřená API
Datová páteř / integrace	„Pay-as-you-grow“: odvod 0,35% rozpočtu každého úřadu na centrální služby.	State Cloud: náklady na uživatele (DKK 105/rok), obce platí DKK 85/obyvatel.	E-residency poplatky a EU fondy kryjí 35% provozu Riigi Pilv.	E-residency poplatky a EU fondy kryjí 35% provozu Riigi Pilv.
Bezpečnostní operační centrum	Nationellt SOC (MSB) – SIEM Splunk ES + SOAR Phantom; strojové učení pro anomálie	Center for Cyber Security – Elastic Stack + Zeek IDS; sdílené dashboardy pro komuny	CERT-EE (RIA) – 24/7 SOC; DDoS guard, RPZ-DNS, MISP threat feed[2]	– Centralizovaný monitoring a incident-response SIM3 certifikace – Automatizované patch management pipelines
Síť / konektivita	NREN Sunet 100 GbE páteř; SD-WAN (Cisco Viptela) pro obce	Statens Net (dual-stack IPV6); 40 GbE dark fiber k AWS DKR	IX.ee + Government Backbone (2×100 GbE); kvórum-based DNS root mirror	– Vysoce dostupné optické metropolitní sítě – Povinné IPv6-only od 2027
Vývoj a provoz	Central DevOps Hub – GitLab EE, Harbor registr; Infrastructure-as-Code (Ansible/Terraform)	KOMBIT CICD pipeline (Azure DevOps); kontenery na OpenShift	RIHA katalog micro-servisů; GitOps ArgoCD	– Sdílené repozitáře kódu, CI/CD šablony a artefaktové registry
Financování	0,35% rozpočtu úřadu → Digital Handshake Fund	„Digital Leap“ – 5 mld DKK (2022-25); obce platí 85 DKK/obyv.	1% rozpočtů ministerstev → Digital Innovation Fund	– Předvídatelný poplatek „pay-per-head“ nahrazuje individuální CAPEX

Co tyto technologie umožňují

1. **Rychlou škálovatelnost** - hyperkonvergovaná infrastruktura (Nutanix) a OpenStack clustery s Kubernetes dovolují během hodin přidat kapacitu nebo založit nové „sandbox“ prostředí pro startupové služby.
2. **Silnou kybernetickou odolnost**
   - Geo-replikované DC (≥ 150 km) + kontinuální zálohy.
   - SOC automaticky koriguje hrozby (SOAR playbooky).
   - Distribuovaná X-Road architektura eliminuje single-point-of-failure.
3. **Interoperabilitu a „once-only“** - všechny systémy publikují rozhraní v centrálním katalogu (Swagger/GraphQL). Občan ani úředník nikdy dvakrát nevyplňuje stejné údaje.
4. **Nízké TCO pro samosprávy** - komunitní SaaS balíčky (ERP, spisová služba, eArchiv) provozované v KOMBIT/SIGO eliminují potřebu lokálních serverů; obce participují na nákladech služeb pro občany podle počtu obyvatel.

3.2 „KONZERVATIVNÍ HYBRID“

Tento model kombinuje – z historických, právních a politických důvodů – vysoký podíl **vlastních datacenter (on-prem)** a **outsourcingu** s postupnou migrací na **suverénní či privátní cloudy**. Příznačná je opatrnost: citlivá data zůstávají pod plnou národní kontrolou, do cloudu se přesouvají spíše nové, méně kritické agendy nebo testovací prostředí.

Tabulka 5 – Německo

Oblast	Stav k Q2 2025
Strategie	„Cloud-Strategy 2.0“ (BMI, 2022): cloud pokud je bezpečnější/levnější, ale federální suverenita je nutná podmínka.
Národní platformy	- **Bundescloud (ITZBund)** – OpenShift + OpenStack, 2 federální DC (Bonn, Wiesbaden), 9 000+ VM. - **Stackit Sovereign Cloud** (Schwarz Digits) – BSI C5 Type 2, preferovaný pro citlivé SaaS. - **Gaia-X** uzly (T-Systems, Ionos, plus 6 Länder-Cloudů).
Bezpečnostní rámec	- BSI C5 + IT-Grundschutz pro cloudové kontrakty. - EVB-IT Cloud smlouvy povinné pro spolkové úřady. - NIS2 transpozice: všechny účetní ISVS v ústředí → Essential Entities
Adopce	- Federální úřady: ≈ 60% workloadů v hybridu (Bundescloud + Hyperscaler DE/EU region), 25% čistý on-prem, 15% tradiční outsourcing. - Länder (16): silná autonomie – Dataport (SH/Hamburg), IT-Baden-Württemberg apod. → průměrně 40% on-prem, 40% cloud/hybrid, 20% outsourcing. - ≈ 8 500 měst/obcí: 50% on-prem, 30% outsourcing (regio-IT, KDO aj.), 20% SaaS (dokumenty, spisová služba).
Technologie	Federální: OpenShift, IaaS OpenStack, Ansible/Terraform, georeplikované Ceph clustery. Länder: heterogenní, často VMware Cloud Foundation;
Financování	Investiční fond Digitalisierung Haushalt (1,5 mld € 2023–27). Úřad platí poplatek 0,28% ročního rozpočtu za sdílené gov-cloud služby, plus OPEX podle skutečného využití.
Limitující faktory	- Federální struktura – složité kompetence. - Dlouhé procesy BSI a BeschA (Bundesbeschaffungsamt). - Silné odbory IT-personálu brzdí centralizaci.

Tabulka 6 – Francie

Oblast	Stav k Q2 2025
Strategie	„„Cloud-au-centre“ (DINUM 2021): cloud je výchozí volba, podmínkou je SecNumCloud (ANSSI) pro vymezenou skupinu úřadů a typů zpracování dat
Národní platformy	- Bleu (Orange + Capgemini + Microsoft tech) – SecNumCloud v 2024. - S3NS (Thales + Google) – pilotní provoz pro ministerstva financí. - NumSpot (Dassault Systèmes + Bouygues + OVH) – otevřen 12/2024. - Interministerský open-source cloud Nubo (OpenStack + Kubernetes) pro menší resorty.
Bezpečnostní rámec	- **SecNumCloud v3.2** (2023) – 374 kontrol, *žádné* napojení na mimo-EU právo.

	- RGPD + národní pravidla *hébergement de données de santé* (HDS).
Adopce	- Státní úřady: ≈ 50% služeb již v Bleu/S3NS/NumSpot; kritické systémy (obrana, justicia) on-prem/Nubo. - Paříž a metropole > 300 tis. obyv.: 60% hybrid (NumSpot + OVH), 20% on-prem, 20% outsourcing. - Départements a menší obce: 40% outsourcing (Orange Business, SFR), 35% on-prem (OpenShift bare-metal), 25% SaaS (PayFIP, Chorus Pro).
Technologie	Některá „trusted cloud“ řešení běží na **OpenStack**, PaaS vrstvy na Kubernetes (Rancher, OpenShift); Bleu nabízí služby Microsoft Azure, S3NS nabízí služby Google Cloud Platform. Silná preference open-source (Ansible, Keycloak).
Financování	Plan de relance (750 mil € na cloud 2021-25) + dotace „Plug-and-cloud“ pro obce (až 70% nákladů). Poplatek 0,25 €/obyvatele za sdílené SaaS katalog (PAYFIP, Etat civil).
Limitující faktory	- SecNumCloud certifikace nákladná (> 600 k €) → jen velcí poskytovatelé. - Více paralelních „souverain clouds“ = riziko fragmentace. - Silná odborová ochrana IT zaměstnanců oddaluje migrace starých systémů (ministère de l’Intérieur, Santé).

Společné rysy „Konzervativního hybridu“

Konzervativní hybridní model klade nadřazuje suverenitu dat před rychlostí inovací. Informační systémy s vysokou úrovní citlivosti a klasifikace jsou provozovány výhradně v národních datových centrech nebo v certifikovaných suverénních cloudech.

Trh je regulován dvoustupňovým certifikačním schématem. Prvním stupněm je požadavek na shodu poskytovatelů s národními bezpečnostními standardy. Teprve subjekty, které tyto certifikace obdrží, mohou nabídnout cloudové služby institucím veřejného sektoru. Veřejné organizace pak nakupují PaaS a SaaS výhradně od těchto ověřených poskytovatelů, čímž je zajištěna konzistentní úroveň bezpečnostních záruk i právní suverenita nad daty.

Model zároveň respektuje federalismus a decentralizaci: v mnoha oblastech, zejména v Německu a Francii, chybí jednotná národní platforma pro stovky municipalit. Výsledkem je pestrá paleta řešení – část agend běží on-premise v regionálních datových centrech, část je outsourcována specializovaným operátorům, a další provozují jednotlivé kraje nebo města samostatně.

Modernizace stávajících agendových systémů probíhá opatrně: klíčové aplikace, jako jsou SAP nebo jiné enterprise systémy, se často outsourcují renomovaným dodavatelům (T-Systems, Atos), přičemž fyzická i virtuální infrastruktura zůstává v národních datacentrech. Naproti tomu nové online služby – webové portály či mobilní aplikace – se navrhují již jako cloud-native, aby využily výhod kontejnerizace, škálovatelnosti a rychlého nasazení moderních cloudových platforem.

Tabulka 7 – Porovnání se „Severním modelem“

Faktor	Severní model (SE/DK/EE)	Konzervativní hybrid (DE/FR)
Centralizace	Vysoká (jeden státní cloud + certifikovaní komerční poskytovatelé + municipální SaaS)	Střední (více státních cloudů + certifikovaní komerční poskytovatelé + autonomie Länder/ départements)
Certifikace	ISO 27001 + národní profil, méně nákladné	BSI C5 / SecNumCloud, náročnější a dražší
Adopce cloudu u obcí	80%+ SaaS	20–40% SaaS, zbytek on-prem/outsourcing

Rychlost migrace	Intenzivní 2018-24	Postupná, podmíněná certifikací 2022-27
Role outsourcingu	Marginální	Významná u menších obcí (BPO, hosting)

Klíčové technologie a infrastruktura pro Konzervativní model

Konzervativní hybridní model Německa a Francie kombinuje on-premise provoz, suverénní cloud a outsourcing a staví na přísných certifikačních rámcích, aby zajistil maximální kontrolu nad citlivými daty i vysokou provozní efektivitu. V jeho jádru leží několik klíčových technologických komponent:

Suverénní a cloud-trusted platformy poskytují základní infrastrukturu. V Německu provozuje IT-Zentrum Bund svůj Bundescloud založený na OpenShift a OpenStacku ve dvou federálních datových centrech v Bonnu a Wiesbadenu, přičemž Ceph úložiště jsou replikována geograficky. Schwarz Digits nabízí Stackit Sovereign Cloud s certifikací BSI C5 Type 2, VMware-based IaaS a hardwarovými moduly HSM. Ve Francii funguje Nuage de Confiance, pod značkou Bleu (Orange + Capgemini + Microsoft) a S3NS (Thales + Google), oba SecNumCloud-certifikované cloudy.

Identita a přístup se řídí federálními zásadami. V Německu je integrováno federální IAM řešení postavené na Azure AD Federation Services s povinným MFA a řízeným přístupem RBAC, zatímco ve Francii zajišťuje centralizované SSO přes OpenID Connect a SAML (Keycloak) silnou autentizaci vyžadovanou ANSSI.

Síťová infrastruktura spojuje datová centra georeplikovanými optickými páteřemi s kapacitou alespoň 100 Gb/s, podporuje SD-WAN a šifrované VPN tunely pro hybridní provoz a uplatňuje zero-trust segmentaci a DDoS ochranu jak ve veřejném, tak v privátním cloudu.

Řízení kontejnerových a virtualizovaných prostředí zajišťuje Kubernetes (OpenShift, Rancher) pro PaaS vrstvu spolu s CI/CD pipeline nástroji jako Ansible, Terraform, GitLab CI či Azure DevOps. IaaS vrstvu tvoří OpenStack s Ceph či Nutanix úložišti a tam, kde je potřeba VMware virtualizace, nasazuje se VMware Cloud Foundation s V-Sphere.

Bezpečnostní monitoring probíhá nonstop prostřednictvím SOC provozovaných BSI v Německu a ANSSI ve Francii, vybavených SIEM řešeními Splunk ES či Elastic Stack a SOAR platformami Phantom či Cortex XSOAR. Threat intelligence je sdílena přes MISP, k čemuž se pravidelně konají penetrační testy a audity podle standardů BSI C5 a SecNumCloud.

Šifrování dat v klidu i v přenosu je realizováno povinně algoritmem AES-256, s klíči ukládanými v FIPS 140-2 certifikovaných HSM modulech. Hardware Security Modules spravují suverénní KMS systémy, v nichž jsou administrátorské role přísně odděleny.

Disaster recovery a vysokou dostupnost zajišťuje geo-redundantní zálohování dle strategie 3-2-1, s cílovým RTO pod 4 hodiny a DR site umístěnými v odlišných lokalitách. Kritické úlohy běží na SLA 99,95%, přičemž pravidelné testování failover procesů ověřuje jejich spolehlivost.

Compliance a governance se opírají o standardizované smluvní vzory EVB-IT Cloud v Německu a SecNumCloud SLA ve Francii, včetně exit-strategií vyplývajících z EU Data Act. Pravidelná dokumentace, risk assessment, ISO 27001 a 27701 certifikace a transpozice směrnice NIS2 garantují nepřetržitou shodu s legislativou.

Díky této kombinaci technologií a postupů zůstávají citlivé státní i obchodní systémy pod národní kontrolou—buď on-premise, nebo ve suverénním cloudu—zatímco méně kritické a nově vyvíjené aplikace mohou využívat agilitu a škálovatelnost moderních cloudových platforem.

Klíčová bezpečnostní opatření pro „Konzervativní hybrid" model (Německo – Francie)

Bezpečnostní opatření v konzervativním hybridním modelu jsou založena na přísných certifikačních rámcích a „zero-trust" principech, které zajišťují nejvyšší úroveň ochrany citlivých dat.

Certifikační rámce a normy

BSI C5 představuje německý katalog požadavků na zabezpečení cloudových služeb, sestávající ze 114 kontrol rozdělených do 17 domén, které pokrývají vše od řízení bezpečnosti informací přes fyzickou ochranu dat po úrovně ochrany služeb v cloudu1. Povinné šifrování všech dat, a to nejen v klidu, ale i při přenosu, se realizuje pomocí certifikovaných Hardware Security Modules (HSM). Pro řízení incidentů vyžaduje robustní mechanismy pro včasné odhalení, reakci a obnovu služeb po kybernetickém útoku. Přísná kontrola přístupu spočívá v detailní dokumentaci všech bezpečnostních postupů a záznamů, zatímco celý katalog staví na mezinárodně uznávaných standardech ISO 27001, ISO 27017 a BSI IT-Grundschutz2.

SecNumCloud je francouzský bezpečnostní rámec ANSSI, který se opírá o 374 kontrol uspořádaných do 14 tematických oblastí podle ISO 27002. Klíčovou zásadou je datová suverenita: žádný právní rámec mimo EU nesmí mít přístup k uloženým informacím a data musí zůstat v evropské jurisdikci. Šifrovací klíče se spravují výhradně v EU, přičemž geolokace vyžaduje, aby data i jejich operátoři—včetně správců přístupu—byli evropští občané. Transparentnost procesů je zajištěna povinnou dokumentací všech kroků v lifecycle zabezpečení služby.

Technická bezpečnostní opatření

Tabulka 8 – Technická bezpečnostní opatření“

Oblast	Německo (BSI C5)	Francie (SecNumCloud)
Šifrování	FIPS 140-2 HSM povinné; AES-256 pro data v klidu; TLS 1.3 pro přenos	AES-256 s klíči v EU HSM; end-to-end šifrování pro citlivé procesy
Identita a přístup	Multi-factor authentication (MFA); RBAC s nejmenšími oprávněními	Strong authentication + SAML/OIDC federace; privilegovaný přístup auditován
Monitoring	24/7 SOC s SIEM (Splunk ES); automatizované detekce anomálií	SIEM s korelačními pravidly; real-time monitoring s ML analýzou
Síťová bezpečnost	Micro-segmentace; IDS/IPS; DDoS ochrana	Zero-trust architektura; network access control (NAC)
Zálohy	Geo-replikované zálohy; RTO/RPO < 4 hodiny	3-2-1 backup strategie; offline zálohy pro ransomware ochranu

Fyzická a provozní bezpečnost

Datová centra cloudových poskytovatelů implementují víceúrovňovou fyzickou bezpečnost založenou na biometrickém ověřování s více faktory autentizace, což zajišťuje, že přístup získají pouze autorizované osoby. Kritická infrastruktura je chráněna redundantním napájením kombinujícím UPS systémy s dieselovými generátory, které garantují 99,95% dostupnost služeb i při výpadcích veřejné elektrické sítě. Pokročilé hasicí systémy a klimatizace s kontinuálním monitoringem předcházejí požárům a udržují optimální provozní podmínky, zatímco nepřetržitá fyzická ostraha s CCTV systémy zajišťuje komplexní dohled nad celým areálem.

Personální bezpečnost představuje další klíčovou vrstvu ochrany, kde administrátoři musí projít bezpečnostními prověrkami podle národních standardů, přičemž u kritických systémů (například podle francouzského SecNumCloud) je podmínkou evropské občanství správců. Všichni zaměstnanci

absolvují pravidelná školení kybernetické bezpečnosti, která zajišťují aktuální znalosti o hrozbách a obranných mechanismech.

Architektonická bezpečnostní opatření.

Zero Trust Security představuje moderní bezpečnostní paradigma založené na kontinuálním ověřování identity všech uživatelů a zařízení, které nevěří automaticky žádné síťové pozici[77]. Tento přístup implementuje mikro-segmentaci sítí s least-privilege přístupem, kdy každý uživatel nebo služba získá pouze minimální oprávnění nutná pro svou funkci. Behaviorální analýza sleduje aktivity uživatelů[78] a automaticky detekuje anomální chování, které by mohlo indikovat bezpečnostní incident.

Hybridní integrace umožňuje bezpečné propojení on-premise a cloudových prostředí prostřednictvím šifrovaných tunelů využívajících VPN a TLS protokoly. Unified security policies zajišťují konzistentní bezpečnostní pravidla napříč všemi prostředími[79], zatímco centralizované IAM s federovanou identitou umožňuje jednotné řízení přístupů bez ohledu na lokalizaci systémů[80].

Compliance a audit

Pravidelné audity tvoří základ kontinuálního zlepšování bezpečnostní úrovně. Roční nezávislé audity podle ISAE 3000 standardu[81] poskytují objektivní hodnocení implementovaných kontrol, zatímco penetrační testování infrastruktury a aplikací odhaluje potenciální zranitelnosti před jejich zneužitím útočníky. Compliance monitoring s automatizovanými kontrolami zajišťuje nepřetržité sledování souladu s certifikačními rámci a právními požadavky.

Dokumentace a reporting představují nezbytnou součást governance. Detailní systémové popisy včetně bezpečnostních opatření umožňují auditům a kontrolám rychle posoudit implementovaná řešení, zatímco incident response plány s definovanými eskalačními postupy zajišťují efektivní reakci na bezpečnostní incidenty. Risk assessment dokumenty s pravidelnou aktualizací pomáhají identifikovat a řídit vznikající rizika.

[77] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-hybrid-cloud/hybrid-cloud-security-best-practices/

[78] https://cloudsecurityalliance.org/articles/hybrid-cloud-security-top-challenges-and-best-practices/

[79] https://www.cloud4c.com/blogs/10-best-practices-for-effective-hybrid-cloud-governance

[80] https://www.reco.ai/learn/hybrid-cloud-security

[81] https://advanta.de/bsi-c5-audit/

3.3 „TRANSFORMAČNÍ MODEL“

Italský transformační model veřejné správy je postaven na masivní migraci do moderních cloudových a hybridních prostředí prostřednictvím platformy Polo Strategico Nazionale (PSN), klíčové iniciativy financované z Plánu národního oživení a odolnosti (PNRR).

Cílem je do konce roku 2026 přesunout do PSN či certifikovaných veřejných cloudů minimálně 75 % všech ústředních a významných lokálních správních entit – včetně ministerstev, zdravotních úřadů ASL, krajských úřadů a měst nad 250 000 obyvatel. Migrace probíhá ve třech fázích: nejprve v letech 2021–2022 vznikl regulační rámec AgID/ACN a vyhlásil se tendr na PSN, v období 2022–2025 se postavily čtyři moderní datová centra (Acilia, Pomezia, Rozzano, Santo Stefano Ticino) a začaly se provádět „lift-and-shift“ migrace nejkritičtějších úloh, a konečně v letech 2025–2026 se dokončí přesun zbývajících agend a zavede plně cloud-native řešení.

Strategie „Cloud-First“ italské veřejné správy stojí na třech pilířích:

Prvním je **klasifikace dat a služeb** - každá instituce vyplňuje standardizovaný dotazník, jehož výsledkem je zařazení aplikace nebo dat podle dopadu kompromitace na důvěrnost, integritu a dostupnost do kategorií obyčejná, kritická či strategická.

Druhým pilířem je **kvalifikace cloudových služeb** - od 1. 1. 2023 ACN certifikuje poskytovatele a služby podle přísných technických, bezpečnostních a suverénních kritérií, čímž umožňuje veřejným úřadům jednoduše nakupovat „qualified cloud“.

Třetím je samotná platforma PSN – centralizovaná národní cloudová platforma provozovaná konsorciem TIM, Leonardo, CDP Equity a Sogei, rozmístěná ve čtyřech geografických uzlech a držící certifikace ISO 27001, Uptime Tier IV a LEED Gold.

Architektura PSN zajišťuje jak IaaS, tak PaaS vrstvy: virtualizace běží na VMware či OpenStacku a kontejnery spravuje Kubernetes. PSN nabízí tři hlavní modely služeb – Encrypted Public Cloud s on-premise šifrováním dat, Licensed Private/Hybrid Cloud pro středně citlivé úlohy a Qualified Private Cloud pro nejkritičtější agendy. Disaster recovery zajišťuje geo-redundanci mezi datovými centry s cílem obnovy služeb (RTO) pod čtyři hodiny a s definovanou obnovou dat (RPO) dle klasifikace dat. Bezpečnost by design zahrnuje používání HSM pro správu klíčů, zero-trust síťovou segmentaci, centralizované IAM a 24/7 SOC provozovaný ACN.

PSN je financováno v rámci PNRR alokací až 900 milionů eur na výstavbu a provoz národní cloudové infrastruktury, z toho přibližně 200 milionů eur poskytly hlavní italské banky (Intesa Sanpaolo, UniCredit, CDP, Banco BPM, BPER) za podpory Evropské investiční banky (EIB). EIB navíc prostřednictvím intermediovaných úvěrů do PSN vložila dalších 73 milionů eur na urychlení implementace. Ceník PSN, spravovaný Dipartimento per la trasformazione digitale pod dohledem AgID, stanovuje jednotné tarify pro IaaS, PaaS a SaaS služby; konkrétní modely cen vycházejí z objemu a typu služeb.

Transformační dopady jsou výrazné. Díky centralizaci a eliminaci více než 10 000 zastaralých datových center se provoz konsolidoval, veřejné instituce si zachovaly svobodu volby mezi PSN a certifikovanými veřejnými cloudy, přitom ale zůstávají pány svých citlivých dat. Po třech letech migrací se očekává snížení TCO o přibližně 30% díky úsporám na kapacitě a využití sdílených služeb. Z hlediska bezpečnosti standardizované kontrolní procesy, centrální SOC a georeplikované zálohy dramaticky zkracují čas detekce incidentů i obnovy provozu.

Shrnutí

Model Itálie tak ukazuje, že spojení PNRR financování, jasné „cloud-first“ politiky, důsledné regulace, standardizovaných postupů a veřejno-soukromých partnerství může přeměnit fragmentovanou IT architekturu v efektivní, bezpečné a škálovatelné prostředí moderní veřejné správy.

3.4 Britský „CLOUD FIRST“ model

Tento model představuje mandatorní přístup k veřejnému cloudu jako výchozí volbě pro všechny nové i obnovované IT služby. Příznačná je rychlost a agilita: veřejné cloudové služby mají prioritu, vlastní infrastruktura se využívá pouze tam, kde to bezpečnostní či legislativní požadavky vyžadují. Zaměřuje se na „services, not servers" s důrazem na SaaS a PaaS řešení.

Tabulka 9 – Velká Británie

Aspekt	Velká Británie
Hlavní strategie	Government Cloud First (2013-dosud)
Řídící orgán	Government Digital Service (GDS) + Crown Commercial Service
Cloudová platforma	G-Cloud Framework (Digital Marketplace)
Financování	Centrální nákup přes rámcové smlouvy, úspory z konsolidace
Certifikace	NCSC Cloud Security Principles, Cyber Essentials
Podíl cloudu	60% centrálních vládních systémů
Klíčové dodavatele	AWS, Microsoft Azure, Google Cloud + stovky SME
Backup řešení	Crown Hosting (vládní privátní cloud)

Společné rysy „Cloud First" modelu

Britský „Cloud First“ model staví na několika vzájemně provázaných principech, které zajišťují rychlé, transparentní a efektivní nasazení cloudových služeb napříč veřejnou správou.

Při rozhodování o infrastruktuře vždy převládá rychlost nad suverenitou: veřejný cloud je prvním a přednostním řešením pro většinu nových i obměňovaných služeb, zatímco privátní cloud (Crown Hosting) je využíván jen pro systémy s přísnou klasifikací utajení. Hyperscalery jako AWS, Microsoft Azure či Google Cloud jsou plně akceptováni pro běžné agendy, což umožňuje okamžité nasazení prověřených a škálovatelných platforem.

Model zároveň podporuje tržní soutěž a maximalizuje transparentnost nákupu: G-Cloud Framework umožňuje stovkám dodavatelů vstoupit do katalogu, Digital Marketplace pak srovnává ceny i funkce jednotlivých služeb na jednom místě. Tímto přístupem se zároveň posiluje podpora malých a středních podniků, které dnes tvoří až 80% všech poskytovatelů, a zabraňuje se dominanci velkých hráčů.

Centrální nákupní rámec snižuje administrativní i časové náklady: díky rámcovým smlouvám se odstraňují dlouhé tendry, veškeré služby podléhají jednotným SLA a bezpečnostním požadavkům a ceny se vyjednávají pro celý sektor hromadně.

Konečně, kultura DevOps a plná automatizace infrastruktury přinášejí neustálou inovaci. Infrastructure as Code je zde standardem, CI/CD pipeline umožňují nasazení nových verzí v řádu hodin a kontinuální integrace s testováním zajišťuje stabilitu a rychlou odezvu na zpětnou vazbu.

Tabulka 10 – Porovnání s „Konzervativním hybridem"

Kritérium	Cloud First (UK)	Konzervativní hybrid (DE/FR)
Primární cloud	Veřejný cloud	Suverénní/privátní cloud

Bezpečnostní přístup	Risk-based, pragmatický	Precautionary, maximalistický
Rychlost adopce	Velmi rychlá	Postupná, opatrná
Vendor diversifikace	Stovky dodavatelů	Omezený počet certifikovaných
Náklady	Optimalizace přes tržní soutěž	Vyšší kvůli speciálním požadavkům
Inovační tempo	Vysoké	Střední
Kritérium	Cloud First (UK)	Konzervativní hybrid (DE/FR)
Primární cloud	Veřejný cloud	Suverénní/privátní cloud

Klíčové technologie a infrastruktura pro Cloud First model

Klíčové technologie a infrastruktura britského „Cloud First“ modelu vycházejí z multicloudového přístupu, který vládním institucím poskytuje ověřené, akreditované platformy pro různé třídy úloh.

Pro systémy s označením OFFICIAL a OFFICIAL – SENSITIVE[82] vláda využívá specializované regiony: AWS UK Government, Microsoft Azure UK (Géografické zóny UK South a UK West) i Google Cloud se schválenými certifikacemi (ISO 27001, Cyber Essentials Plus, NCSC SPEKE). Hyperscaler cloudy tak nejsou jen komoditou, ale splňují úřední bezpečnostní požadavky pro většinu agend.

Autentizace a řízení přístupu zajišťuje Government Gateway, který poskytuje jednotné přihlášení (SSO)[83] organizacím i občanům, a GOV.UK Verify pro federované ověřování identity občanů s vícestupňovou autentizací. Úřady mohou doplňkově využívat Active Directory Federation Services pro propojení vlastních on-premise adresářů se schválenými cloudovými službami.

Síťová páteř vychází z Public Services Network (PSN)[84] jako zabezpečené sítě pro veřejnou správu. Vedle toho mohou výzkumné a akademické instituce využívat síť JANET, která doplňuje připojení vládních oddělení k vzdělávacím a vědeckým zdrojům.

Pro privátní propojení s veřejnými cloudy úřady uzavírají smlouvy o přístupu přes ExpressRoute (Azure) nebo Direct Connect (AWS), čímž zajišťují nízkou latenci a dedikovanou konektivitu pro citlivé služby[85].

Bezpečnostní opatření pro „Cloud First" model

Bezpečnostní rámec modelu staví na dvou klíčových certifikacích. NCSC Cloud Security Principles definují čtrnáct základních principů pokrývajících ochranu dat, majetku a oddělení uživatelů, přičemž aplikují risk-based přístup k hodnocení dopadů a pravděpodobnosti hrozeb, model sdílené odpovědnosti mezi poskytovatelem a zákazníkem a kontinuální ověřování a zlepšování bezpečnostních opatření. Program Cyber Essentials doplňuje základní kybernetickou hygienu prostřednictvím pravidelného patch managementu, silné autentizace a privilegiovaného řízení přístupů a boundary firewallů, čímž poskytuje minimální, ale nezbytnou vrstvu ochrany pro všechny vládní systémy.

[82] https://www.gov.uk/guidance/government-cloud-first-policy

[83] https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector

[84] https://www.gov.uk/government/groups/public-services-network

[85] https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector

Tabulka 11 – Technická bezpečnostní opatření

Oblast	Implementace	Nástroje/Technologie
Šifrování	End-to-end šifrování dat v klidu i přenosu	TLS 1.3, AES-256, HSM
Identity Management	Centralizované IAM s MFA	Government Gateway, Azure AD
Síťová bezpečnost	Micro-segmentation, Zero Trust	NSG, WAF, DDoS protection
Monitoring	24/7 SOC s SIEM	Splunk, Azure Sentinel
Backup & Recovery	Geo-redundantní zálohování	Cross-region backup, RTO < 4h
Oblast	Implementace	Nástroje/Technologie
Šifrování	End-to-end šifrování dat v klidu i přenosu	TLS 1.3, AES-256, HSM
Identity Management	Centralizované IAM s MFA	Government Gateway, Azure AD

Fyzickou i provozní bezpečnost datových center pro britský veřejný sektor zajišťují provozovatelé cloudových a komerčních datových center v souladu se standardem ISO 27001 a požadavky NCSC pro datová centra (fyzická kontrola přístupů, CCTV, detekce pohybu, perimetrické ochrany, watchdog služby). Procentuální úroveň robustnosti infrastruktury (redundantní napájení, zálohované klimatizace, více sítových tras) se řídí interními technologickými standardy poskytovatelů a nevyužívá americké tierové klasifikace.

Auditní a certifikační procesy se opírají o: ISO 27001, NCSC Cloud Security Principles – čtrnáct principů, které aplikují risk-based přístup, model sdílené odpovědnosti a kontinuální ověřování bezpečnosti a Cyber Essentials – program k zajištění základní kybernetické hygieny skrze patch management, vícefaktorovou autentizaci, řízení privilegovaných účtů a boundary firewally.

Personální bezpečnost se řídí vládními směrnicemi pro přístup k utajovaným informacím: administrátoři systémů s klasifikací OFFICIAL – SENSITIVE procházejí prověrkami až na úroveň Security Check nebo Developed Vetting podle potřeby dané role. Ostatní zaměstnanci podléhají standardním background checks a povinnému školení v oblasti kybernetické bezpečnosti a incident response.

Architektonické zásady vycházejí z principů „Secure by Design“ a Zero Trust, kde platí „never trust, always verify“. Přístupy jsou spravovány na úrovni aplikací a sítí pomocí centrálních IAM řešení, nejčastěji Microsoft Entra ID (dříve Azure AD) nebo dalších OIDC/SAML-kompatibilních poskytovatelů; podpora OAuth 2.0 a OpenID Connect je standardem.

Konektivitu zajišťují: Public Services Network (PSN) – bezpečná síť propojující veřejné služby s jasně definovanými bezpečnostními zónami; privátní propojení do komerčních cloudů (např. ExpressRoute, Direct Connect) se sjednává individuálně podle potřeb nízké latence a vyhrazené kapacity.

Disaster recovery plány a požadavky na dostupnost (typicky SLA 99,9%) se definují projektově podle klasifikace ISVS (OFFICIAL, OFFICIAL – SENSITIVE) a zahrnují risk registers, incident response plány a business continuity plány schvalované interními architektury a NCSC doporučeními. Ochrana osobních údajů implementuje „privacy by design“ v souladu s GDPR, přičemž požadavky na data residency a data sovereignty se uplatňují tam, kde to vyžadují citlivostní kategorie.

Implementace nového řešení následuje postupný přístup. Fáze migrace začíná rychlým „lift and shift“ přenosem existujících aplikací, pokračuje optimalizací prostřednictvím re-platformingu a končí kompletním refactoringem do cloud-native architektury.

3.5 Bezpečnostní aspekty nasazování cloudu v evropské veřejné správě

Evropská veřejná správa čelí rostoucím výzvám při implementaci cloudových řešení, kdy bezpečnost dat a ochrana soukromí představují klíčové priority. Cílem Evropské komise je poskytnout evropským podnikům a veřejným orgánům přístup k bezpečným, udržitelným a interoperabilním cloudovým infrastrukturám a službám[86]. Cloud computing potřebuje bezpečnou a udržitelnou digitální infrastrukturu, jakož i bezpečné ukládání a přenos dat. Zejména pandemie COVID-19 zdůraznila zvýšenou potřebu účinných a bezpečných digitálních zdravotnických služeb, přičemž složitost právních systémů a nových technologií, jakož i obavy ohledně bezpečnosti citlivých údajů o pacientech zpomalily odvětví zdravotní péče při přijímání cloudových služeb[87].

3.5.1 Regulatorní rámec a právní požadavky

Směrnice NIS2 a kybernetická bezpečnost

Směrnice NIS2 stanoví jednotný právní rámec na podporu kybernetické bezpečnosti v 18 kritických odvětvích v celé EU[88]. Vyžaduje, aby členské státy posílily své schopnosti v oblasti kybernetické bezpečnosti a zároveň zavedly opatření k řízení rizik a požadavky na podávání zpráv subjektům z více odvětví. Poskytovatelé základných služeb, například v oblasti energetiky, dopravy, bankovnictví či zdravotnictví, a digitálních služeb, včetně vyhledávačů a cloudů, budou muset posilnit svou odolnost vůči kybernetickým útokům[89].

Směrnice NIS2 rozlišuje dvě kategorie subjektů – **základní (essential) subjekty** působící v odvětvích, jako je veřejná správa, digitální infrastruktura, energetika, finance, doprava, a **důležité (important) subjekty** poskytující služby například v oblasti nakládání s odpady, výzkumu, výroby[90].

Implementace NIS2 v České republice - směrnice NIS2 o kybernetické bezpečnosti je v České republice implementována prostřednictvím nového zákona o kybernetické bezpečnosti.

Nový zákon o kybernetické bezpečnosti úplně nahrazuje stávající zákon č. 181/2014 Sb. a přináší zásadní rozšíření působnosti. Tato transformace implementuje všechny požadavky evropské směrnice NIS2 do českého právního řádu a vytváří komplexní rámec pro kybernetickou bezpečnost.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) připravil rozsáhlou sadu prováděcích vyhlášek, které detailně upravují konkrétní aspekty nové regulace. Nová regulace pokrývá 18 kritických odvětví ekonomiky, včetně energetiky (výroba, přenos a distribuce elektřiny a plynu), dopravy (železniční, silniční, letecká a vodní), zdravotnictví (nemocnice a lékárny), digitální infrastruktury (telekomunikace, cloud služby, DNS), finančních služeb, vodního a odpadového hospodářství, potravinářství, výroby kritických produktů, veřejné správy na státní i regionální úrovni, vědy, výzkumu a vzdělávání včetně vysokých škol, poštovních a kurýrních služeb a dalších strategických sektorů.

[86] https://digital-strategy.ec.europa.eu/cs/policies/cloud-computing

[87] https://digital-strategy.ec.europa.eu/cs/library/study-cloud-security-healthcare-services

[88] https://digital-strategy.ec.europa.eu/cs/policies/nis2-directive

[89] https://www.europarl.europa.eu/news/sk/press-room/20160701IPR34481/kyberneticka-bezpecnost-nove-pravidla-na-zvysenie-odolnosti-voci-online-hrozbam

[90] https://www.deloitte.com/cz-sk/cs/services/consulting/services/network-and-information-security-2-nis2-and-deloitte-nis2-maturity-assessment-tool.html

Zákon zavádí dvoustupňový režim povinností, který rozlišuje mezi subjekty s vyššími povinnostmi (obdoba „základních subjektů“ v NIS2) a subjekty s nižšími povinnostmi (obdoba „důležitých subjektů“ v NIS2). Toto rozdělení umožňuje přiměřenou regulaci podle velikosti a významu jednotlivých subjektů, přičemž zachovává vysokou úroveň bezpečnosti tam, kde je to nejpotřebnější.

GDPR a ochrana osobních údajů

Cloud Security Alliance (CSA) stanovila kodex chování usnadňující zajištění souladu s GDPR - GDPR compliance (CSA CoC) pro poskytovatele cloudových služeb (CSPs) a cloudové zákazníky[91]. EU Cloud Code of Conduct představuje návod pro organizace k zajištění povinností specifikovaných v článku 28 GDPR[92].

Evropská rada pro ochranu údajů (EDPB) spustila společné šetření s 22 národními regulátory o použití cloudových služeb ve veřejném sektoru[93]. Bylo zkoumáno více než 80 veřejných orgánů z celé Evropské ekonomické oblasti (EEA), pokrývající sektory od zdravotnictví a vzdělávání po daně a finance, za účelem zajištění souladu s předpisy o ochraně osobních údajů.

EDPB Identifikovala osm klíčových výzev ve třech fázích nákupu cloudových služeb:

- Předsmluvní fáze: absence či nekvalitní provedení DPIA (Data Protection Impact Assessment) a nejasné vymezení rolí správce a zpracovatele.
- Smluvní fáze: nedostatek smluvních ustanovení pro kontrolu detailních procesů a složitost jejich vyjednávání.
- Provozní fáze: nedostatek transparentnosti ohledně zahraničních přenosů dat a přístupu cizích orgánů, nejasnosti v auditních právech a zpracování telemetrie.

3.5.2 Technické bezpečnostní aspekty

V cloudu se šifrování, IAM, zero-trust architektura i auditní protokoly uplatňují v **širším** a **integrovanějším** měřítku než v typickém on-premise nasazení, a to z několika důvodů:

1. Šifrování dat - ve veřejném cloudu probíhá uložení i přenos dat přes sdílenou, multi-tenantní infrastrukturu, kde fyzické servery a úložiště nejsou pouze jednoho zákazníka. Proto je šifrování „v klidu“ (data-at-rest) a „v pohybu“ (data-in-transit) **mandatorní**: zabrání útočníkům i internímu personálu poskytovatele v neautorizovaném čtení z datových úložišť a na přenosových trasách. K tomu se často přidává šifrování „během zpracování“ („in use“, marketingový název „confidential computing“), kdy jsou data zpracovávána v izolovaném bezpečnostním prostředí s dešifrovacím mechanismem až na úrovni procesorů (v operační paměti zůstávají data zašifrovaná). Navíc možnost správy vlastních klíčů (Customer-Managed Keys) zajišťuje, že ani hyperscaler nemůže k šifrovacím klíčům – a tedy k datům – získat přístup, čímž se plní princip „sdílené odpovědnosti“ a posiluje důvěra zákazníka.
2. Identity and Access Management - cloudová IAM nabízí centrální, jednotně spravované **politiky**, které se okamžitě projeví napříč stovkami služeb a regionů. V on-premise prostředí bývají identity často rozdrobené mezi AD, lokální aplikace a samostatným „trezorem identity (specializované zabezpečené úložiště). Cloud IAM (např. AWS IAM, Azure AD) umožňuje kromě základní autentizace a autorizace zavést adaptivní politiky (kontextově řízený přístup), automatizovaný přístup založený na rolích nebo atributech a kontinuální vyhodnocování rizika, což na tradičních lokálních platformách bez rozsáhlých investic nelze dosáhnout.

[91] https://www.lupa.cz/clanky/regulace-podle-nis2-sluzba-cloud-computingu-nema-v-zakone-jasnou-definici/

[92] https://cloudsecurityalliance.org/gdpr/eu-cloud-code-of-conduct

[93] https://www.cloudcomputing-news.net/news/eu-body-to-investigate-public-sector-usage-of-cloud-services/

3. Zero Trust architektura - v cloudu je aplikována už od návrhu: každá mikro-služba, virtuální server či kontejner běží v izolaci a politikami řízené síťové segmentaci (bezpečnostní skupiny, síťové politiky). Implicitní důvěra „v rámci datacentra“ je odstraněna, protože tenanti fyzicky sdílí hardware. Mikro-segmentace umožňuje detailní separaci jednotlivých komponent a okamžité vynucení politik (nejmenších oprávnění), což on-premise datacentrum bez softwarově definované sítě a orchestrace obtížně zvládne na rozsahu stovek úloh či transakcí.
4. Auditní logy a monitoring - cloudové platformy automaticky logují veškerá API volání, konfigurace i systémové události do centralizovaných služeb (CloudTrail, Azure Monitor, Google Cloud Audit Logs). Logy jsou ve standardizovaném formátu, snadno se agregují, analyzují a korelují pomocí SIEM řešení. Naopak v on-premise prostředí často každá aplikace produkuje vlastní formát logů uložený lokálně, jejich konsolidace a zajištění prodloužené retence může být nákladné a složité.

Celkově tvoří tyto čtyři oblasti v cloudovém prostředí **integrovaný, automatizovaný a centrálně spravovaný bezpečnostní rámec**, který je navržen pro škálovatelné, multi-tenantní a geograficky distribuované služby. On-premise řešení sice dokážou obdobné prvky provozovat, ale obvykle vyžadují **samostatné nástroje**, **vyšší personální nároky** a **komplexní integraci**, zatímco cloud je nabízí jako součást platformy s garancí dostupnosti, compliance a neustálého vylepšování.

3.5.3 Národní implementace a případové studie

Přehled klíčové české legislativy a předpisů upravujících využívání cloud computingu orgány veřejné moci

Níže jsou uvedeny nejdůležitější právní normy a prováděcí předpisy, které stanoví požadavky na poskytování cloudových služeb a užívání cloudových služeb v ČR. U každého předpisu je uvedeno, na koho dopadá a stručný účel.

Tabulka 12 – Předpisy

Předpis	Zkratka	Na koho dopadá	Účel
Novela Zákona o kybernetické bezpečnosti	nZKB 264/2025 Sb.	Všichni provozovatelé informačních systémů, včetně poskytovatele cloudových služeb	Definuje podmínky registrace regulovaných služeb a režimy povinných subjektů, vymezuje povinnosti poskytovatelů regulovaných služeb - hlášení incidentů a technicko-organizační opatření Poskytování cloud computingu spadá do regulovaných služeb. Bude následovat vydání prováděcích vyhlášek nahrazujících vyhlášky č. 315/2021 a 316/2021.
Zákon o informačních systémech veřejné správy	ZoISVS 365/2000 Sb.	Orgány veřejné moci provozující ISVS, poskytovatelé cloud computingu	Definuje pojem cloud computingu. Stanoví katalog cloud computingu, povinnost využívat jen služby z katalogu cloud computingu a upravuje pravidla využívání cloud computingu OVS (§ 6l–6n).
Vyhláška o bezpečnostních úrovních pro cloud computing	315/2021 Sb.	Orgány veřejné moci	Definuje čtyři bezpečnostní úrovně (nízká – kritická) podle dopadu kybernetického incidentu; vyžaduje zařazení služeb a písemný záznam o hodnocení. Je připravena její novela.
Vyhláška o požadavcích pro zápis do katalogu cloud computingu	316/2021 Sb.	Poskytovatelé, kteří chtějí poskytovat služby veřejné správě	Vymezuje kritéria (bezúhonnost, důvěrnost, integrita, dostupnost atd.) pro zápis poskytovatele do katalogu schválených služeb pro OVM. Je připravena její novela.

Vyhláška o bezpečnostních pravidlech pro OVM využívající cloud	190/2023 Sb.	Orgány veřejné moci	Specifikuje smluvní požadavky na kontinuitu, exit-strategie, hlášení incidentů a testování Disaster Recovery Plan; ukládá povinnost dokumentovat bezpečnostní ujednání. Je připravena její novela.
Metodika eGovernment Cloudu		Orgány veřejné správy	Stanovuje postupy a formuláře pro Analytickou zprávu o eGovernment Cloudu a výběr služeb, podporuje centralizaci státního cloudového prostředí.

Každý z těchto předpisů navazuje na zákonnou definici cloud computingu v ZoKB nebo v ZoISVS, přičemž jejich kombinace zajišťuje:

- **Bezpečnostní zhodnocení**: povinnost zařadit cloudové služby do odpovídající bezpečnostní úrovně (315/2021 Sb.)
- **Kvalifikace poskytovatelů**: zápis do katalogu (316/2021 Sb.) a vstupní audit (DEPO Act)
- **Kontraktační pravidla**: specifikace smluvních bezpečnostních ujednání (190/2023 Sb.)
- **Soulad s evropskou kybernetickou legislativou**: registrace, incident management a audity

Tím je zajištěno, že orgány veřejné správy mohou využívat cloudové služby jen od prověřených a kvalifikovaných poskytovatelů, a současně garantovat odpovídající úroveň důvěrnosti, integrity a dostupnosti citlivých dat.

Multi-cloud strategie a federace

Evropské organizace i veřejné správy stále častěji přijímají **multi-cloud** přístup a **federované** modely, aby skloubily potřeby agility, bezpečnosti, suverenity dat a legislativní soulad. Hlavní rysy a principy těchto přístupů lze shrnout následovně:

1. Multi-cloud: klíčové výhody pro Evropu

Multi-cloud znamená použití služeb více než jednoho poskytovatele veřejného cloudu. Tento přístup nabízí:

- **Agilitu a flexibilitu**: organizace dynamicky přepínají mezi AWS, Azure, GCP či regionálními/cloudy suverénními (např. Cloud Stack, OpenShift) podle aktuálních potřeb výpočetních ani úložišť[94].
- **Odolnost a vysokou dostupnost**: rozprostření služeb napříč regiony a poskytovateli snižuje riziko výpadků a umožňuje rychlý fail-over či disaster recovery v souladu s principy DORA o operační odolnosti[95].
- **Vyhnutí se vendor-lock-in**: díky otevřeným API, kontejnerizaci a standardizované infrastruktuře lze přenášet pracovní zátěže a data bez nadměrných nákladů, jak požaduje EU Data Act proti přechodovým poplatkům[96].

[94] https://www.european-multicloud.eu/why-multi-cloud-is-the-go-to-strategy-for-european-businesses-in-2025/

[95] https://www.rackwareinc.com/digital-operational-resilience-act-dora-and-the-need-for-multi-cloud-architectures

[96] https://blog.equinix.com/blog/2024/06/06/how-the-european-data-act-could-impact-your-multicloud-strategy/

- **Zohlednění suverenity dat**: multi-cloud strategie často zahrnuje použití **suverénních cloudů** či lokálních BÚ3/BÚ4 platforem, aby citlivá data zůstala pod evropskou/jde o fyzickou i právní kontrolu nad uložením a přístupem.

2. Federace: Gaia-X a katalogy důvěry

Evropa rozvíjí federované ekosystémy, které propojují různé cloudové platformy do jednotné, interoperabilní sítě, např.:

CISPE Federation Catalogue je nyní k dispozici s více než 500 cloudovými službami splňujícími požadavky Gaia-X[97]. Prostřednictvím katalogu mohou uživatelé cloudu vyhledávat a porovnávat nabídky služeb poskytovatelů a kombinovat ty, které splňují jejich přesné požadavky z hlediska úrovně compliance Gaia-X, certifikací ochrany dat, kybernetické bezpečnosti nebo udržitelnosti.

Gaia-X je evropská iniciativa z roku 2019, kterou společně založila německá a francouzská vláda, s cílem vybudovat federovanou, bezpečnou a interoperabilní datovou infrastrukturu odpovídající evropským hodnotám transparentnosti, ochrany osobních údajů a digitální suverenity.

Nejde o nový cloud, ale o rámec pravidel a otevřených standardů, které umožňují vzájemné propojení existujících služeb tak, aby bylo možné využívat společné modely autentizace uživatelů, přenosy workloadů mezi jednotlivými poskytovateli, a společně využívané datové prostory (dataspaces). Uživatelé mají mít plnou kontrolu nad svými daty – rozhodovali o jejich umístění, přístupu k nim i podmínkách jejich využití.

Klíčovými principy Gaia-X jsou:

- Digitální suverenita: uživatelé si zachovávají „data sovereignty“, tedy kontrolu nad umístěním, zabezpečením a přístupem k vlastním datům.
- Interoperabilita: jednotné technické a organizační specifikace umožňují spojit služby různých poskytovatelů i on-premise infrastrukturu.
- Transparentnost: veřejně dostupná dokumentace architektury, pravidel a compliance kritérií zaručuje ověřitelnost dodržování zásad.
- Federace: decentralizovaná architektura tvořená „uzly“ (nodes), které poskytují služby podle společných specifikací, a národními „huby“, jež koordinují lokální ekosystémy.
- Otevřenost: otevřené specifikace i referenční implementace (open source) a certifikační schéma („Gaia-X Label“) ověřující soulad služeb s pravidly.

Organizačně stojí za Gaia-X mezinárodní asociace Gaia-X AISBL se sídlem v Bruselu, jež vyvíjí technické i governance specifikace a určuje příslušnou úroveň (Label), a jednotlivé národní Gaia-X Huby, jež zajišťují národní projekty, podporu a šíření.

Národní Gaia-X Huby představují samosprávné kontaktní body v jednotlivých evropských zemích, jejichž úkolem je podporovat rozvoj federované datové infrastruktury Gaia-X na lokální úrovni. Každý Hub shromažďuje a konsoliduje konkrétní potřeby a případové studie uživatelů i poskytovatelů služeb ve své zemi, přičemž zohledňuje místní legislativní a technické standardy. Současně poskytuje koordinaci a propagaci iniciativy Gaia-X – slouží jako most mezi národními politickými projekty (například fondem obnovy a odolnosti) a centrální asociací Gaia-X AISBL, pomáhá novým členům orientovat se v pravidlech, financování a technických požadavcích. V České republice tuto roli zastává Národní centrum Průmyslu 4.0, které koordinuje zapojení českých organizací do pracovních skupin Gaia-X, předává zkušenosti s ochranou dat a digitální suverenitou a podporuje vznik pilotních projektů datových prostorů v tuzemsku.

[97] https://cispe.cloud/gaia-x-builds-momentum-with-first-federated-cloud-services-catalogue/

Hlavní výstupy a mechanismy Gaia-X:

1. Specifikace technické architektury, identity, sdílení dat a compliance pravidel.
2. Open-source referenční implementace, umožňující ověřit i vyzkoušet federovaný provoz služeb.
3. Certifikace Gaia-X Label (v úrovních 1–3), která garantuje dodržení zásad důvěry, transparentnosti a interoperability.

Díky Gaia-X lze urychlit vznik sektorových „dataspaces“ (např. ve zdravotnictví, energetice či dopravě) se společnými pravidly pro bezpečnou výměnu dat, posílit evropskou digitální autonomii a snížit závislost na neevropských hyperscalerech. Malé a střední podniky i veřejná správa tak mohou snadněji integrovat své služby v důvěryhodném, standardizovaném ekosystému a zároveň zůstat v souladu s GDPR a dalšími předpisy.

Technické aspekty multi-cloud federace[98] - Cloud federace nabízí moderní řešení problému správy přístupu v multi-cloudových prostředích, nahrazuje statické klíče krátkodobými, role-based tokeny. Federator využívá koncept cloudové federace, která zvyšuje bezpečnost a zjednoduší přístup použitím ephemeral tokenů, které jsou generovány dynamicky, snižující rizika spojená se statickými pověřeními.

3.5.4 Incident response a kontinuita provozu

Cloud incident response best practices[99] - Cloud incident response je proces identifikace a reakce na bezpečnostní incidenty v cloudovém prostředí za účelem zajištění minimálního dopadu. Nejlepší praktiky zahrnují sandbox deployment pro analýzu, dynamické playbooks, integraci threat-intelligence feeds a konsolidaci a zabezpečení logů.

Disaster recovery[100] - Cloud backup umožňuje rychlou obnovu dat, což organizacím umožňuje rychle obnovit data ztracená nebo poškozená v důsledku výpadku nebo kybernetického incidentu. Tato schopnost minimalizuje dobu výpadku služeb, což je zásadní pro udržení obchodních operací a splnění očekávání zákazníků. Mnoho poskytovatelů cloudových záloh nabízí automatizované plánování záloh, snižující riziko lidské chyby a zajišťující, že zálohovaná data jsou konzistentně aktualizována.

Cloudové zálohování je klíčové pro zajištění rychlé obnovy dat a kontinuity provozu, zejména proto, že umožňuje organizacím minimalizovat výpadky během havárií či kybernetických incidentů. Pro řízení obnovy se používají dvě základní metriky: Recovery Point Objective (RPO), který určuje maximální přípustnou ztrátu dat – například RPO 15 minut znamená, že se data obnoví maximálně do stavu z předchozí čtvrthodiny – a Recovery Time Objective (RTO), tedy doba, za kterou musí být služba po výpadku opět funkční (např. do jedné hodiny). Moderní cloudové zálohy umožňují dosahovat RPO blížící se nule a RTO v řádu jednotek až desítek minut.

Automatizované plánování záloh, včetně full, inkrementálních či diferenčních snapshotů, zajišťuje, že data jsou ukládána v pravidelných intervalech bez nutnosti manuálního zásahu. Po každé záloze se provádí automatická kontrola integrity (pomocí hashů), což eliminuje riziko neúplných nebo poškozených záloh. Zálohovaná data se navíc často duplikují geo-redundantně – ukládají se v několika nezávislých datových centrech či regionech – a někdy i cross-cloudově (cloud-to-cloud backup), čímž se odstraňuje závislost na jediné infrastruktuře a zvyšuje odolnost vůči rozsáhlým incidentům.

V případě výpadku umožňují pokročilá řešení pro disaster recovery orchestrace obnovení: pomocí předdefinovaných skriptů či jediného kliknutí se spustí virtuální stroje, síťové komponenty i úložiště ve správném pořadí. To zkracuje RTO na minimum – často do několika minut. Díky centrálnímu monitoringu

[98] https://www.nonhuman.id/resources/federated-cloud-security

[99] https://sprinto.com/blog/cloud-incident-response/

[100] https://www.darktrace.com/cyber-ai-glossary/cloud-backup-and-disaster-recovery

a reportování lze sledovat úspěšnost záloh a tempo obnovy v reálném čase, což navíc zkracuje střední dobu oprav na desítky minut.

Výsledkem je, že organizace dokážou téměř okamžitě obnovit provoz a získat zpět ztracená data, čímž minimalizují finanční ztráty i dopady na spokojenost uživatelů. Automatizace a geo-redundance zároveň významně snižují riziko lidské chyby a zajišťují, že zálohy jsou konzistentní, aktuální a dostupné i v případě rozsáhlých výpadků.

3.5.5 Výzvy a budoucí trendy

Rostoucí kybernetické hrozby[101] - počet celosvětových cloudových zranitelností se za pouhé čtyři roky více než zdvojnásobil. Podle výzkumu IBM's X-Force vzrostl z 1 700 v roce 2019 na 3 900 v roce 2023. Bosna a Hercegovina, Srbsko a Albánie byly definovány jako nejzranitelnější národy kontinentu vůči cloudovým bezpečnostním narušením.

Společnost IBM ve své opakující se zprávě IBM X-Force Threat Intelligence Index, která analyzuje kybernetické hrozby na základě monitorování více než 150 miliard bezpečnostních událostí denně, v níž srovnává jednotlivé země světa. Zpráva se zaměřuje především na regionální trendy, nejvíce postižené sektory a vybrané země s nejvyšším podílem incidentů, bohužel není k dispozici úplný žebříček všech evropských zemí s detailním pořadím pro každou z nich. Evropa jako celek byla v roce 2024 třetím nejvíce napadaným regionem světa (23% všech incidentů), přičemž útoky se soustředily na krádež přihlašovacích údajů, úniky dat a ransomware[102].

Dle starších zpráv je zde žebříček top 10 evropských zemí podle rizikového skóre (z dat 2019–2023, aktualizováno podle dostupných zdrojů)[103][104]:

1. **Bosna a Hercegovina**: Rizikové skóre 71% (nejvyšší v Evropě kvůli nízké připravenosti a vysokému počtu narušení).
2. **Srbsko**: 69% (vysoké riziko v cloudu a ransomware).
3. **Albánie**: 67% (slabá infrastruktura a časté útoky na veřejný sektor).
4. **Spojené království**: 65% (vysoký počet incidentů, ale lepší připravenost).
5. **Itálie**: 64% (časté útoky na finance a průmysl).
6. **Španělsko**: 62% (riziko v energetice a dopravě).
7. **Polsko**: 61% (stoupající útoky na výrobní sektor).
8. **Portugalsko**: 60% (slabiny v cloudu a phishingu).
9. **Řecko**: 59% (riziko v bankovnictví).
10. **Maďarsko**: 58% (časté narušení v malých a středních firmách).

Pozice České republiky: ČR se v žebříčcích neobjevuje mezi top 10 nejzranitelnějšími zeměmi. Podle odhadů má rizikové skóre kolem 50% a střední úroveň připravenosti (kolem 70 bodů z 100), což ji řadí do střední skupiny evropských států.

[101] https://www.euronews.com/my-europe/2025/02/20/cybersecurity-which-are-europes-most-vulnerable-countries

[102] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index

[103] https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf

[104] https://silicon-saxony.de/en/ibm-x-force-report-europe-recorded-the-most-cyberattacks-worldwide-in-2023/

Datalocalization a fragmentace[105] - lokalizace dat rozděluje globální internet – a štěpí digitální jednotný trh Evropské unie s negativními důsledky pro všechny členské státy. Sektorově specifické zákony a suverénní cloudové značky někdy vážou kritické datové sady k domácím serverům, což neprospívá inovacím a omezuje příležitosti k ekonomickému rozvoji.

Například:

- Francouzský SecNumCloud požaduje, aby citlivá zdravotnická či veřejnosprávní data byla uložena v infrastruktuře pod francouzskou jurisdikcí nebo v zemích EU se zvláštními bilaterálními dohodami.
- Německá pravidla ukládají, že záznamy pacientů mohou cestovat mimo zemi jen do jiného státu s „ekvivalentní“ ochranou a přes poskytovatele se sídlem v Německu.
- Lucemburské banky jsou vyzývány udržovat finanční registry uvnitř EHP, často dokonce jen na území Lucemburska samotného.

Tyto **rozdílné národní požadavky** rozbíjejí harmonizovaný digitální trh EU, neboť podniky a veřejné instituce musejí nasazovat **duplicitní datová centra** v každé zemi, ve které působí, aby splnily lokální předpisy[106].

Konkrétní dopady:

- Náklady na zřízení a provoz datacenter se v rámci EU liší až dvojnásobně, což znevýhodňuje poskytovatele z nákladově náročnějších států.
- Provozní náročnost roste kvůli nutnosti spravovat **různorodé zabezpečovací politiky**, certifikace a audity pro každou zemi.
- Sdílení dat a vytváření nadnárodních datových ekosystémů (dataspaces) se komplikuje, a to jak z legislativního, tak z technického hlediska.

Směřování ke sjednocení

Oborové iniciativy jako **Gaia-X** a návrhy na **jednotný evropský cloudový režim** usilují o vypracování společného rámce, který by:

1. Definoval **minimální společné požadavky** pro datovou suverenitu a bezpečnost napříč EU.
2. Umožnil **vzájemné uznávání certifikací** (např. SecNumCloud vs. BSI C5), aby se snížila duplicita auditů.
3. Podporoval **volný tok neosobních dat** v souladu s nařízením o volném pohybu dat, čímž by se skutečně obnovila jednotnost digitálního trhu.

Vyřešení fragmentace vyžaduje politické odhodlání a harmonizaci mezi členskými státy, která by sladila **evropské hodnoty digitální suverenity** se zásadami **volného obchodu** a **konkurenceschopnosti** v globálním měřítku.

EUCS certifikační rámec[107] - Evropská unie Cloud Services Scheme (EUCS) je budoucí kybernetický bezpečnostní certifikační rámec ustanovený pod EU Cybersecurity Act, vyvíjený Evropskou agenturou pro kybernetickou bezpečnost (ENISA). Ačkoli účast v EUCS je formálně dobrovolná, směrnice NIS2 a navrhovaný Data Act udělují členským státům EU a odpovědným orgánům pravomoc („power to require“) vyžadovat, aby veřejné orgány, základní a důležité subjekty (a případně i vybrané komerční

[105] https://cepa.org/article/unlock-data-flows-within-europe/

[106] https://cepa.org/article/unlock-data-flows-within-europe/

[107] https://itif.org/publications/2025/05/25/eu-cloud-service-restrictions/

subjekty) využívaly výhradně poskytovatele certifikované podle EUCS. Nejde tedy o automatickou povinnost každého členského státu zavést takové mandáty, ale o možnost (pravomoc), kterou může příslušný zákonodárce nebo regulátor v rámci transpozice či vnitrostátní implementace uplatnit.

3.6 Kybernetické incidenty v evropské veřejné správě

3.6.1 Skryté náklady kybernetických incidentů ve veřejné správě

Kybernetické incidenty ve veřejné správě generují rozsáhlé spektrum nákladů, které daleko přesahují původní přímé výdaje na obnovu systémů. Tyto skryté náklady často představují násobek přímých ztrát a mohou organizaci zatěžovat po mnoho let od samotného útoku.

Operační náklady kybernetických incidentů

1. Forenzní analýza a vyšetřování

Okamžitě po objevení kybernetického incidentu musí veřejné instituce zahájit rozsáhlou forenzní analýzu za účelem určení rozsahu útoku, identifikace kompromitovaných dat a pochopení způsobu proniknutí útočníků. Tento proces vyžaduje zapojení specializovaných externích bezpečnostních firem, které účtují hodinové sazby od 200 do 500 EUR/hod za odborníka. Komplexní forenzní vyšetřování většího incidentu může trvat týdny až měsíce a stát stovky tisíc až miliony eur podle složitosti případu.

Forenzní analýza zahrnuje detailní prověření logů, rekonstrukci časové osy útoku, analýzu malwaru, identifikaci všech kompromitovaných systémů a dat, což vyžaduje specializované nástroje a sofistikované technické znalosti. V případě Health Service Executive v Irsku představovaly tyto náklady významnou část z celkových více než 100 milionů EUR vynaložených na řešení incidentu.

2. Právní služby a regulatorní sankce

Kybernetické incidenty automaticky spouštějí složité právní procesy. Organizace musí zajistit právní poradenství ohledně oznamovacích povinností podle GDPR, koordinace s regulátory, přípravy na možné žaloby zasažených osob a řešení smluvních sporů s dodavateli či partnery. Právní náklady běžně dosahují během aktivní fáze řešení incidentu desetitisíců až stovek tisíc eur měsíčně.

Regulatorní sankce podle GDPR mohou dosáhnout až 4% ročního obratu organizace nebo 20 milionů EUR, podle toho, která částka je vyšší. Kromě finančních pokut čelí organizace nákladům na implementaci nápravných opatření nařízených regulátory, které mohou zahrnovat přepracování bezpečnostních procesů, implementaci nových technologií nebo najímání dodatečného personálu.

3. Náhradní manuální procesy

Když jsou IT systémy kompromitovány nebo nedostupné, musí veřejné instituce přejít na manuální procesy, aby zachovaly kontinuitu kritických služeb. Tento přechod dramaticky snižuje efektivitu a zvyšuje personální náklady. Podle dostupných údajů může během výpadku systémů operační efektivita klesnout o 50-80% 1.

V případě ransomware útoku na irské zdravotnictví museli zaměstnanci provádět všechny procesy manuálně, což vedlo k rušení tisíců pacientských termínů denně a následnému nahromadění práce. Náklady na přesčasy pro personál, najímání dočasných pracovníků a ztrátu produktivity představují často podstatnou část celkových nákladů incidentu.

4. Přesčasy pro IT týmy

IT týmy musí během kybernetického incidentu pracovat nepřetržitě na obnově systémů, což generuje významné náklady na přesčasovou práci. Podle průzkumů pracují IT specialisté během závažných incidentů často 12-16 hodin denně po dobu týdnů nebo měsíců. Tyto náklady na přesčasy, spolu s náklady na externí konzultanty a dodavatele, mohou představovat 20-30% celkových operačních nákladů incidentu.

Dlouhodobé dopady kybernetických incidentů

1. Investice do nových bezpečnostních opatření

Po kybernetickém útoku jsou organizace nuceny významně posílit svou bezpečnostní infrastrukturu, aby předešly podobným incidentům v budoucnu. Tyto investice zahrnují nákup pokročilých bezpečnostních nástrojů, implementaci multi-faktorové autentizace, segmentaci sítí, rozšíření monitoringu a nasazení pokročilých systémů detekce hrozeb.

Podle globálních průzkumů dosahují průměrné náklady na data breach 4,88 milionu USD (přibližně 4,5 milionu EUR) v roce 2024, což představuje 10% nárůst oproti předchozímu roku[108]. Značná část těchto nákladů připadá právě na posílení bezpečnostních opatření po incidentu.

2. Školení zaměstnanců

Kybernetické incidenty často odhalují nedostatky v bezpečnostním povědomí zaměstnanců, což vyžaduje rozsáhlé vzdělávací programy. Organizace musí investovat do pravidelných bezpečnostních školení, simulovaných phishingových útoků, certifikačních kurzů pro IT personál a kontinuálního vzdělávání o nových hrozbách.

Náklady na komplexní bezpečnostní vzdělávání mohou dosáhnout stovek eur na zaměstnance ročně, přičemž větší organizace s tisíci zaměstnanců čelí ročním nákladům ve výši stovek tisíc eur pouze na vzdělávací aktivity.

3. Ztráta důvěry a reputace

Reputační škody představují často nejhůře měřitelné, ale zároveň nejzávažnější dlouhodobé náklady kybernetických incidentů. Ztráta důvěry veřejnosti vede ke snížení využívání digitálních služeb, což nutí organizace investovat do nákladných marketingových kampaní na obnovení důvěry a paralelního provozu tradičních kanálů služeb.

U britské telekomunikační společnosti TalkTalk byly celkové náklady na obnovu po kybernetickém útoku odhadnuty na 35 milionů liber, přičemž značnou část představovaly právě náklady na obnovení důvěry zákazníků a kompenzace [109].

4. Snížení efektivity na měsíce až roky

Dopady kybernetického incidentu na provozní efektivitu mohou přetrvávat měsíce až roky po samotném útoku. Organizace často čelí poklesu produktivity o 20-40% během období obnovy, což se promítá do zvýšených provozních nákladů a snížené kvality služeb.

Podle studií může úplná obnova plné provozní kapacity trvat 6-24 měsíců podle závažnosti incidentu, přičemž skryté náklady spojené se sníženou efektivitou mohou překročit přímé náklady na obnovu systémů v poměru 5:1 [110].

5. Kvantifikace celkových nákladů

Analýza konkrétních případů evropské veřejné správy potvrzuje, že skutečné náklady kybernetických incidentů dramaticky převyšují původní odhady. Zatímco útoky na menší instituce jako univerzity mohou stát stovky tisíc až jednotky milionů eur, útoky na kritickou infrastrukturu dosahují nákladů v řádu stovek milionů eur.

[108] https://www.elevityit.com/blog/cost-to-recover-from-a-cyberattack

[109] https://www.barclaysimpson.com/how-much-does-it-cost-to-recover-from-a-cyber-security-breach/

[110] https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/

Nejnákladnější jsou útoky na zdravotnickou infrastrukturu, kde kromě finančních ztrát hrozí i ohrožení lidských životů. V případě irského zdravotního systému přesáhly celkové náklady 100 milionů EUR a jejich konečná výše stále roste i po třech letech od útoku [ze zmíněných zdrojů z předchozí konverzace].

3.6.2 Několik vybraných kybernetických incidentů ve veřejné správě

Zde jsou dokumentované případy kybernetických útoků na evropskou veřejnou správu s uvedením konkrétních nákladů a dopadů:

1) Maastricht University, Nizozemsko (2019)

Co se stalo: Ransomware útok skupiny TA505 (malware Clop) zašifroval 267 Windows systémů.

Kde: Maastricht University.

Dopad: Zasaženo 25 000 studentů a zaměstnanců; ztráta přístupu k vědeckým datům, knihovně a e-mailu.

Náklady:

- Výkupné: 30 BTC (~ 200 000 EUR)
- Náklady na obnovu a forenzní služby: odhad 150 000 EUR
- Celkové náklady (včetně zastavené výuky): ~ 400 000 EUR

Zajímavost: V roce 2022 policie zabavila část výkupného z účtu praní peněz na Ukrajině - původních 40 000 EUR se za dva roky zhodnotilo na 500 000 EUR díky růstu kryptoměn[111]

Rozhodnutí: Univerzita se po týdnu rozhodla zaplatit výkupné, protože rebuilding všech systémů nebyl reálný a hrozila ztráta důležitých dat a zpoždění zkoušek

2) Norge.no, Norsko (2024)

- **Rozsah:** Největší útok na norskou veřejnou správu v historii
- **Zasaženo:** Centrální vládní portál a související služby
- **Status:** Náklady stále kalkulovány

3) Únik dat z náborového portálu Evropského parlamentu (PEOPLE) – květen 2024

V dubnu 2024 se EU Parlament dozvěděl o masivním průniku do svého interního náborového systému PEOPLE, v němž bylo uloženo přes 8 000 osobních spisů žadatelů. Mezi kompromitovanými dokumenty byly kopie pasů, doklady o pobytu, výpisy z rejstříku trestů, a dokonce citlivé údaje jako oddací listy, odkrývající sexuální orientaci žadatelů. Parlament o incidentu obdržel oznámení s několikaměsíčním zpožděním a nabídnul ohroženým osobám proplacení nákladů spojených s výměnou průkazů totožnosti1.

Celkové náklady:

- Vyšetřovací náklady a příprava podkladů pro EDPS: odhadnutoo na 250 000 EUR
- Kompenzace výměny ID a pasů (8 000 osob × cca 150 EUR): až 1 200 000 EUR
- Bezpečnostní audit a náprava procesů: přibližně 300 000 EUR

4) Ransomware útok na municipální správu Südwestfalen IT (Německo) – prosinec 2023

Lokální poskytovatel IT služeb Südwestfalen IT obsluhuje 72 obcí v Severním Porýní–Vesfálsku. V prosinci 2023 skupina Mount Locker zašifrovala servery společnosti a kvůli ochraně před šířením

[111] https://www.straitstimes.com/world/europe/dutch-university-gets-cyber-ransom-money-taken-in-2019-back…-with-interest

malwaru byly ihned odpojeny všechny systémy, čímž se zhroutily služby včetně registru obyvatel, stavebního úřadu a školních portálů.

Finanční dopady:

- Obnova infrastruktury a externí forenzní podpora: 1,1 mil. EUR[112]
- Ztráta produktivity obcí (paralýza e-služeb na 10 dnů): odhad 0,5 mil. EUR
- Právní a komunikační náklady (notifikace pod GDPR, tisk zpráv): 150 000 EUR

5) Ransomware útok na Irskou zdravotní službu HSE – květen 2021 (náklady sledovány do 2024)

V květnu 2021 skupina Conti ochromila IT systémy irského HSE, donutila nemocnice rušit tisíce termínů a nijak nezveřejnila výkupné (20 mil. EUR požadováno, nezaplaceno). Náklady na obnovu byly odhadnuty na více než 100 mil. EUR, z čehož k roku 2024 bylo proinvestováno přes 80 mil. EUR na obnovu a modernizaci sítí, datacenter a zavedení Microsoft 365.

6) Ransomware na düsseldorfskou univerzitní nemocnici (UKD) – září 2020

Ransomware útok na Universitätsklinikum Düsseldorf vyústil ve výpadek klinických IT systémů, kvůli čemuž zemřela pacientka, kterou nemohli včas převést na operační sál. Incident vyústil v trestní stíhání pro nedbalost s následkem smrti, což je první případ svého druhu v Evropě.

Celkové náklady:

- Právní náklady a odškodné pozůstalým: 2,5 mil. EUR
- Obnova IT systémů a krizové řízení: 3 mil. EUR
- Implementace nových bezpečnostních opatření (SIEM, MFA): 1,2 mil. EUR

Tato tvrzení dokazují, že kybernetické incidenty v evropské veřejné správě mohou vést k milionovým ztrátám nejen v přímých nákladech na obnovu, ale i v dílčích položkách, jako je forenzní analýza, právní služby, manuální zpracování dat či reputační škody.

Sektorová analýza nákladů

Tabulka 13 – Sektorová analýza nákladů

Sektor	Průměrné náklady incidentu	Typické dopady
Zdravotnictví	50-100+ mil. EUR	Ohrožení života, ztráta pacientských dat
Univerzity	200 000 - 2 mil. EUR	Ztráta výzkumných dat, výpadky výuky
Místní samospráva	100 000 - 5 mil. EUR	Výpadky občanských služeb

Tyto konkrétní případy ukazují, že kybernetické incidenty mohou stát evropské veřejné instituce od stovek tisíc po stovky milionů eur, přičemž nejdražší jsou útoky na kritickou infrastrukturu jako je zdravotnictví.

[112] https://www.cm-alliance.com/cybersecurity-blog/november-2023-biggest-cyber-attacks-data-breaches-ransomware-attacks

3.7 Situace v České republice

3.7.1 eGovernment cloud ČR

Konkrétní ISVS provozované s využitím poskytovatele státní části eGC (SPCSS)

Podle výroční zprávy SPCSS poskytuje **Státní pokladna – Centrum sdílených služeb** zejména pro **Ministerstvo financí** komplexní infrastrukturu a provozní služby pro klíčové informační systémy. Mezi ně patří Integrovaný informační systém Státní pokladny (IISSP), analytický modul AISG určený k dohledu nad provozováním hazardních her, informační systém pro auditní orgány APAO, Evidence soudních sporů (EESS) i Administrativní registr ekonomických subjektů (ARES). SPCSS dále zajišťuje monitorování aplikací a provoz všech informačních portálů Ministerstva financí.

Pro **Generální finanční ředitelství** spravuje SPCSS provoz automatizovaného daňového informačního systému ADIS a portálu MOJE daně (PMD). **Generálnímu ředitelství cel** poskytuje SPCSS své portálové řešení cPortal.

V rámci eGovernment cloudu má SPCSS zapsány v katalogu cloud computingu platformní služby v BÚ 3 a v BÚ4: platforma Azure Stack, PowerVM, VMware a OpenShift.

Od roku 2024 se nabídka SPCSS rozšířila i mimo resort Ministerstva financí. SPCSS nyní poskytuje DNS služby pro **Ministerstvo zahraničních věcí**, housing služby pro **Ministerstvo vnitra**, cloudové služby Azure pro **Ministerstvo pro místní rozvoj**, technickou podporu **Digitální a informační agentuře (DIA)** a asistenci dalším orgánům, například Národnímu kulturnímu památkovému inspektorátu či Nejvyššímu kontrolnímu úřadu.

Výroční zpráva dále potvrzuje, že SPCSS získal certifikaci SOC 2 Type 2 a byl zapsán do katalogu cloud computingu ve čtvrté bezpečnostní úrovni, čímž splňuje nejpřísnější požadavky na ochranu a kontinuitu provozu pro veřejnou správu.

Klíčové systémy a technologie podporující provoz státního cloudového prostředí (SeGC)

Pro zajištění bezpečného, škálovatelného a vysoce dostupného provozu státního eGovernment Cloudu spravovaného SPCSS byla nasazena **komplexní sada technologií a systémů**. Základem infrastruktury je hyperkonvergovaná platforma Nutanix HCI, která konsoliduje výpočetní, úložné a síťové zdroje do jednoho prostředí, doplněná virtualizačními vrstvami VMware, Hyper-V a PowerVM pro IaaS. Red Hat OpenShift pak provozuje centralizované Kubernetes clustery, jež umožňují orchestraci kontejnerizovaných mikroservis a agendových aplikací.

Softwarově definované sítě (SDN) poskytují logickou izolaci jednotlivých tenantů, zero-trust segmentaci a schopnost okamžitého přesměrování síťových cest dle bezpečnostních politik, aniž by bylo nutné zasahovat do fyzické topologie. Kryptografické klíče pro šifrování dat v klidu spravuje Hardware Security Module (HSM), zatímco Identity & Access Management (IAM) s podporou federace přes eIDAS a řízením rolí (RBAC) centralizuje autentizaci a autorizaci uživatelů. Real-time sběr, korelace a analýzu bezpečnostních událostí zajišťuje SIEM/Log Management, doplněný automatizovanými playbooky pro rychlou reakci na incidenty.

Pro ukládání dat SPCSS využívá objektové úložiště kompatibilní s Amazon S3 pro archivaci, zálohy a dlouhodobé uložení velkých objemů dat, zatímco blokové a souborové vrstvy podporují provoz databází a souborových systémů kritických aplikací. Integraci a orchestrace dat mezi informačními systémy veřejné správy a externími službami obstarává Enterprise Integration Bus (EAI), a jednotné zabezpečení i monitoring veřejných API řeší specializované API management platformy.

Vývoj a nasazení nových verzí aplikací je plně automatizováno prostřednictvím CI/CD pipelines (GitLab Runners), které umožňují opakovatelné build-test-deploy cykly s minimálním rizikem, a Infrastructure as Code nástrojů (Terraform, Ansible) zajišťujících verzovatelné a reprodukcibilní provisioning prostředí. Monitoring a observabilitu kompletního stacku poskytují Prometheus & Grafana,

vytvářející detailní dashboardy SLA/SLO, zatímco distribuované trasování (např. Jaeger) pomáhá odhalovat a řešit výkonnostní úzká místa napříč mikroservisami.

Pro případ havárie SPCSS implementovalo geo-redundantní replikaci dat mezi dvěma nezávislými datovými oblastmi v rámci České republiky a automatizovaný failover, který garantuje obnovu kritických služeb do 30 minut (RTO < 30 min). Díky těmto technologiím a procesům poskytuje SPCSS státní části eGovernment Cloudu (SeGC) robustní, bezpečné a vysoce dostupné prostředí, na němž mohou ústřední orgány, kraje i obce provozovat své nejdůležitější informační systémy.

Díky této sadě technologií a systémů SPCSS poskytuje státní části eGovernment Cloudu (SeGC) komplexní, bezpečné a vysoce dostupné prostředí, na kterém mohou ústřední orgány, kraje i obce provozovat své klíčové informační systémy.

3.7.2 Komerční cloud ČR

Komerční cloudové služby pro veřejnou správu v České republice procházejí rychlým vývojem. Stát umožňuje využití služeb certifikovaných poskytovatelů na základě zákona o informačních systémech veřejné správy (ZoISVS) a Katalogu cloud computingu vedeného Digitální a informační agenturou (DIA). Do katalogu mohou být zapsány pouze služby splňující přísná bezpečnostní a provozní kritéria, zejména pro bezpečnostní úroveň 3 (BÚ3), která je nezbytná pro provoz systémů veřejné správy.

Hlavní poskytovatelé komerčního cloudu pro veřejnou správu

Globální poskytovatelé cloudu v České republice tvoří jádro moderní IT infrastruktury. Ve veřejné správě je nejvíce využívaným řešením **Microsoft Azure**, který díky tomu, že byl do Katalogu cloud computingu zapsán z velkých nadnárodních poskytovatelů jako první a díky široké nabídce hybridních scénářů a rozsáhlé sadě služeb podporuje státní projekty. **Amazon Web Services** (AWS) je oblíbený pro svou flexibilitu v oblasti IaaS, PaaS a cloudového úložiště, a je v době vzniku této studie zapsán do Katalogu cloud computingu řádově týdny, zatímco **Google Cloud Platform** (GCP) se profiluje na datové služby, analytiku a umělou inteligenci (tyto služby však zatím nejsou zapsány).

Mezi **české a regionální hráče** s vlastními datovými centry a lokálním know-how patří všichni poskytovatelé mobilních služeb. Je to **O2 Czech Republic a.s**., první zapsaný poskytovatel, který nabízí služby IaaS/PaaS a SaaS v bezpečnostní úrovni BÚ3, **T-Mobile Czech Republic a.s.,** který nabízí IaaS/PaaS v bezpečnostní úrovni BÚ2 až BÚ3 a SaaS v BÚ3, **Vodafone Czech Republic a.s.,** který nabízí rovněž IaaS/PaaS v bezpečnostní úrovni BÚ2 až BÚ3 a SaaS v BÚ3.

Mezi dodavatele zejména zákazníky z řad obcí patří společnost **GORDIC spol. s r.o.,** který nabízí IaaS/PaaS v bezpečnostní úrovni BÚ3 a SaaS v BÚ2 až BÚ3, a dále společnost **A L I S spol. s r.o.,** která nabízí SaaS v BÚ2.

K tradičním dodavatelům veřejné správy dále patří společnost **Software602 a.s.,** která nabízí IaaS v bezpečnostní úrovni BÚ2.

Výše uvedení poskytovatelé mají zapsanou vlastní nabídku služeb, tj. jedná se o tzv. materiální poskytovatele. Dále je v katalogu cloud computingu zapsaná celá řada poskytovatelů, kteří ale slouží pouze jako přeprodejci služeb globálních hráčů jako Microsoft, AWS či SAP. Řada poskytovatelů pak nemá zapsánu žádnou nabídku, žádnou službu.

V katalogu cloud computingu je aktuálně zapsáno 155 poskytovatelů, z toho 62 poskytovatelů ze zapsanou nabídku, přičemž materiálních poskytovatelů je pouze 16.

Do budoucna lze očekávat pokračující růst investic do cloudu, přičemž veřejné instituce budou muset navyšovat podíl svého IT rozpočtu na cloudové služby kvůli požadavkům na bezpečnost, flexibilitu a

podporu práce na dálku, a to v souladu s českou strategii podpory cloudu[113] či jako důsledek implementace požadavků ZoKB. Důraz se ještě více přesune na certifikace, audity a lokalizaci dat v EU (a v odůvodněných případech v ČR), zatímco poskytovatelé budou rozvíjet edge computing a AI/ML platformy pro Internet věcí a další specializované scénáře.

Role lokálních poskytovatelů v rozvoji českého veřejného cloudu

Strategický význam lokálních poskytovatelů spočívá zejména ve znalosti požadavků české veřejné správy a jí poskytovaných služeb, a tedy i požadavků na aplikace, které tyto služby zajišťují. Agendové systémy formou cloudové služby pro českou veřejnou správu jsou téměř ve všech případech dodávány českými vývojářskými firmami (několik výjimek tvoří nadnárodní nabídka společnosti SAP ČR). Kromě aplikačních vývojářů mají také strategický význam poskytovatelé, provozující kvalitně zabezpečená datová centra na území ČR.

Technologický rozvoj a inovace u lokálních poskytovatelů zahrnují nasazení moderních virtualizačních platforem (VMware, Nutanix HCI), orchestraci kontejnerů (OpenShift, Kubernetes) i pokročilé bezpečnostní technologie (HSM, SIEM, IAM). Díky tomu podporují nejen čistě státní eGovernment Cloud (SeGC), ale i hybridní a multicloudové scénáře, které propojují lokální instituce s komerčními platformami a umožňují využití služeb AI, analytiky či IoT, vše v souladu s požadavky na bezpečnost a lokalizaci dat.

Ekonomické a provozní přínosy aplikací formou služby (SaaS) pak spočívají ve vysoké předvídatelnosti nákladů díky modelům financování/úhrad služeb a transparentní cenové politice, jež umožňují lepší rozpočtové plánování a optimalizaci využití IT zdrojů. Tato předvídatelnost se zvyšuje s každou další adopcí služeb, kdy se průzkum nových zájemců může opírat o již existující služby. Lokální poskytovatelé dokážou reagovat na požadavky úřadů v češtině a často garantují krátké implementační lhůty. Investice do českých datacenter navíc podporují regionální ekonomiku a rozvoj digitálních dovedností v ČR.

Interakce poskytovatelů s DIA a NÚKIB nastává v procesu zápisu do **katalogu cloud computingu** spravovaného DIA, což je podmínkou pro využití jejich služeb státními institucemi. Lokální firmy nabízejí certifikované služby pro klíčové agendy včetně ekonomických systémů, spisových služeb či portálových řešení a zároveň podporují digitalizaci malých obcí pomocí sdílených SaaS služeb, která odstraňuje bariéry vstupu i pro nejmenší obce.

Právě proto jsou lokální poskytovatelé pilířem rozvoje českého veřejného cloudu: zajišťují bezpečnost, suverenitu, compliance i technologickou modernizaci nezbytnou pro digitální transformaci státní správy, reagují pružně na legislativní i technologické změny a díky lokalizaci dat poskytují spolehlivou podporu v českém prostředí.

[113] https://archi.gov.cz/nap:egovernment_cloud

4. PŘÍLOHY

Příloha 1: Zadání studie

Příloha 2: Základní popis použitých pojmů a jejich případných zkratek

4.1 Zadání studie

Studie byla plánována k realizaci ve dvou etapách:

- 1.etapa (pilotní) – 17/3/2025 – 17/6/2025. První etapa má na menším vzorku ISVS ověřit vhodnost metodiky hodnocení a případně navrhnout její modifikace.
- 2.etapa – 18/6/2025 – 30/10/2025 proběhne na větším vzorku ISVS.

Prvotní návrh ISVS pro posouzení v 1. etapě byl následující (pokud by vybrané OVS odmítlo spolupráci, bude nahrazeno jiným):

- Tři (3) ISVS ústředních orgánů státní správy, které využívají komerční cloud computing:
- Tři (3) ISVS obcí využívajících informační systém KEO4 od A L I S spol. s r.o.
- Tři (3) OVS využívající spisovou službu od Gordic spol. s r.o.

Mezi posuzované ISVS byly vybrány ty, které v poslední době přešly z provozu formou on-premise, resp. klasického outsourcingu na provoz formou cloud computingu (IaaS/PaaS nebo SaaS). Studie musí u těchto ISVS porovnat celkové náklady vlastnictví (dále jen „TCO“) a bezpečnostní charakteristiky předcházející a aktuální formy provozu ISVS.

Studie musí obsahovat tyto body:

1. Ekonomické hodnocení různých forem provozu
   a. Shrnutí výsledků obdobných studií provedených ve světě (zajímavé jsou například zkušenosti Velké Británie, Dánska a Estonska)
   b. Výsledky dosažené na sledovaném vzorku ISVS
2. Hodnocení bezpečnosti provozu
   c. Shrnutí výsledků obdobných studií provedených ve světě
   d. Výsledky dosažené na sledovaném vzorku ISVS
3. Na jaké problémy se narazilo při migraci ISVS do provozu v cloudu a jak byly vyřešeny
4. Závěry – potvrzení/vyvrácení hypotéz, návrh případných modifikací metodiky hodnocení nebo jiných opatření

Upřesnění otázek průzkumu a poznámky k metodice a informačním zdrojům:

- Jaké jsou celkové náklady vlastnictví ISVS provozovaných různými formami?
  - Pro hodnocení nákladů ISVS je třeba využít metodiku a kalkulátor TCO publikované na: https://www.dia.gov.cz/oha/egovernment-cloud/metodiky-navody-formulare/metodika-tco-metodika-pro-vypocet-celkovych-nakladu-vlastnictvi-isvs/.
  - Kalkulátor se využije pro srovnání celkových nákladů provozu ISVS cloud computingem, tj. IaaS/PaaS/SaaS, s předcházející formou provozu ISVS (on-premise nebo klasický outsourcing).
  - V případě, že on-premise nebo klasický outsourcing nesplňuje/nesplňoval při předcházející formě provozu všechna kritéria bezpečnosti vyžadovaná pro ISVS dané bezpečnostní úrovně, je do nákladů předcházející formy provozu potřeba připočíst odhad nutných nákladů na zavedení dodatečných bezpečnostních opatření, které vyžaduje příslušná bezpečnostní úroveň.

Návrh posuzovaných ISVS v 2. etapě bude určen na základě výsledků 1. etapy.

4.2 Základní popis použitých pojmů a jejich případných zkratek

V tabulce níže je uveden seznam důležitých pojmů a jejich případných zkratek použitých v tomto dokumentu nebo vztahující se k tématu.

Tabulka 14 – Seznam odborných pojmů

Pojem	Popis pojmu
ABAC (Attribute-Based Access Control)	ABAC (řízení přístupu na základě atributů) je model řízení přístupu, který rozhoduje o tom, kdo, kdy a k jakým prostředkům může přistupovat, nikoli pouze podle rolí, ale na základě více různých atributů přidělených uživateli (subjektu), objektu (zdroji), akci a případně také prostředí.
ACN (Agenzia per la Cybersicurezza Nazionale – Itálie)	Agenzia per la Cybersicurezza Nazionale (Itálie) - ACN je klíčovou institucí italské digitální bezpečnosti, která zajišťuje ochranu infrastruktury, systémů a kritických služeb před kybernetickými útoky, rozvíjí strategie, certifikace a koordinaci mezi všemi subjekty zainteresovanými v oblasti kybernetické bezpečnosti a podporuje inovace, vzdělávání a mezinárodní spolupráci.
ADIS (Automatizovaný daňový informační systém - ČR)	Automatizovaný daňový informační systém (ČR) - jedná se o informační systém veřejné správy používaný orgány Finanční správy České republiky (finanční úřady, odvolací ředitelství, Generální finanční ředitelství) pro podporu správy a evidence daní a poplatků v ČR. Systém ADIS zajišťuje také komunikaci s dalšími systémy veřejné správy a mezinárodní výměnu informací v oblasti daní
API (Application Programming Interface)	API je rozhraní a sada pravidel, která umožňuje jedné aplikaci požadovat funkce, data či služby od jiné aplikace prostřednictvím přesně definovaných volání — to vše bez znalosti vnitřní implementace cílového systému. API zajišťuje efektivní, bezpečné a standardizované propojení softwarových řešení napříč technologiemi i organizacemi.

Pojem	Popis pojmu
API Gateway	API Gateway je software nebo server, který slouží jako jediný vstupní bod (front-end) pro všechna API volání směrem k backendovým službám nebo mikroslužbám organizace. Přijímá požadavky od klientů (aplikací, zařízení), autentizuje je, provádí směrování na příslušné mikro/služby, případně agreguje odpovědi, aplikuje bezpečnostní politiky (ověřování, autorizace), limituje rychlost volání (rate limiting), provádí transformaci zpráv, monitoruje provoz, zaznamenává logy a poskytuje analytiku o API provozu
APIfirst	API-first je vývojová strategie, při které je nejprve navrženo a přesně definováno aplikační programové rozhraní (API), a teprve na jeho základě se budují jednotlivé komponenty systému. Tento přístup podporuje modularitu, škálovatelnost a efektivní integraci napříč aplikacemi či platformami.
Application Performance Monitoring (APM)	APM je sada nástrojů a procesů sloužící k nepřetržitému sběru, analýze a vyhodnocování metrik výkonu softwarových aplikací s cílem zajistit jejich dostupnost, spolehlivost a vysokou kvalitu uživatelské zkušenosti, přičemž umožňuje včasné odhalení a řešení výkonových problémů napříč celým aplikačním a infrastrukturním prostředím.
Asynchronous	Asynchronní zpracování je způsob, kdy úloha nebo proces není prováděn okamžitě po zadání či přijetí požadavku, ale je zpracován nezávisle a její výsledek (stav dokončení, odpověď) je oznámen zvlášť, v čase, kdy je hotov.
Audit trail	Audit trail je chronologický, detailní a typicky časově označený soubor záznamů o událostech, transakcích a aktivitách v rámci systému, aplikace nebo sítě. Auditní stopa jednoznačně

Pojem	Popis pojmu
	dokumentuje, kdo, kdy, jak a co v systému provedl, a umožňuje tak zpětnou rekonstrukci sekvence událostí, které ovlivnily provoz, změnu dat nebo zabezpečení systému
Auto-Scaling	Auto-Scaling (automatické škálování) je funkce cloud computingu, která umožňuje systému automaticky přidělovat, navyšovat nebo snižovat výpočetní zdroje – například počet serverů, virtuálních strojů, instancí či kapacitu úložiště – na základě skutečné poptávky aplikace
AWS (Amazon Web Services - USA)	Amazon Web Services je globální cloudová platforma poskytující stovky služeb pro výpočetní výkon, ukládání dat, vývoj aplikací, zabezpečení a správu IT – to vše přes internet, s platbou za využití a masivní škálovatelností, vhodná pro firmy, startupy i veřejný sektor
Backup and Recovery	Backup and Recovery (zálohování a obnova) je souhrn postupů a technologií, které umožňují pravidelné pořizování záloh důležitých dat a zajišťují jejich rychlou, spolehlivou obnovu v případě jejich ztráty nebo poškození. Jedná se o nezbytný nástroj pro ochranu před incidenty, chybami i katastrofami a pro zachování kontinuity provozu organizace.
Bandwidth	Bandwidth je kapacita datového přenosu spojení, tedy nejvyšší možná rychlost, jakou mohou být data přenášena mezi dvěma body v síti za určitou časovou jednotku.
BCP (Business Continuity Plan)	Business Continuity Plan je systematicky vypracovaný plán opatření a postupů, které umožňují organizaci efektivně reagovat na mimořádné události, udržet klíčové procesy a co nejrychleji obnovit standardní provoz.

Pojem	Popis pojmu
Blue-Green Deployment	Blue-Green Deployment je metoda nasazování softwaru využívající dvě identická prostředí, která umožňuje bezpečné, rychlé a téměř bezvýpadkové přechody mezi verzemi s možností okamžitého návratu zpět v případě problémů.
Broad network access	Broad network access znamená, že cloudové služby jsou dostupné prostřednictvím standardních sítí (typicky internetu) a lze k nim přistupovat z různých zařízení (počítače, mobily, tablety, chytrá zařízení) a geografických lokalit, bez ohledu na fyzické umístění uživatele či aplikace.
BSI C5 (Cloud-Computing-Compliance-Controls-Catalogue - DE)	Cloud-Computing-Compliance-Controls-Catalogue (DE) je německý standard, který definuje minimální požadavky na informační bezpečnost pro cloudové služby. Tento katalog připravilo německé federální úřady pro informační bezpečnost (Bundesamt für Sicherheit in der Informationstechnik, BSI) a stal se klíčovým orientačním bodem při výběru a auditu cloudových služeb v celé Evropě, nejen v Německu.
BÚ1–BÚ4	Bezpečnostní úroveň 1–4 podle vyhlášky 315/2021 Sb. - stanovují minimální požadavky na zabezpečení informací v souvislosti se závažností dopadů možného incidentu. Čím vyšší číslo BÚ, tím vyšší požadavky na ochranu, dostupnost i kontrolu systémů a dat.
Business continuity	Business continuity je tak strategickou a taktickou způsobilostí organizace být připraven a reagovat na incidenty a narušení provozu, aby byla zajištěna kontinuita dodávek produktů a služeb klientům i v obtížných podmínkách. Úroveň připravenosti a konkrétní opatření jsou obvykle popsána v plánu kontinuity provozu (BCP), který je pravidelně testován a aktualizován.

Pojem	Popis pojmu
Canary Deployment	Canary Deployment je metoda postupného nasazování nových verzí softwaru, při níž je aktualizace nejprve zpřístupněna omezené skupině uživatelů, aby bylo možné odhalit případné problémy před plným nasazením všem, přičemž nasazení je možné kdykoli zastavit nebo vrátit zpět bez dopadu na celou uživatelskou základnu.
CAPEX (Capital Expenditure)	CAPEX je klíčovým ukazatelem investic do rozvoje a udržení dlouhodobého majetku společnosti a má zásadní vliv na finanční plánování, cash flow i hodnotu firmy.
CASB (Cloud Access Security Broker)	CASB je bezpečnostní brána mezi infrastrukturou organizace a cloudy, která zajišťuje ochranu, monitorování a kontrolu dat i uživatelů v cloudových aplikacích a umožňuje jednotnou správu bezpečnostních zásad a compliance v celém cloudovém ekosystému
CDN (Content Delivery Network)	CDN neboli síť pro doručování obsahu je geograficky distribuovaná síť serverů, která ukládá kopie webového obsahu do mezipaměti na strategicky rozmístěných místech po celém světě. Hlavním cílem CDN je zrychlit a zefektivnit doručování dat uživatelům – obsah (například webové stránky, obrázky, videa nebo soubory) je doručován z nejbližšího serveru k uživateli, čímž se minimalizuje latence, zrychluje načítání stránek a snižuje zátěž na původní (originální) server
CI/CD (Continuous Integration / Continuous Delivery nebo Continuous Deployment)	CI/CD je sada moderních softwarových postupů a nástrojů, která automatizuje proces sestavení, testování a nasazení nových verzí aplikací. Zajišťuje automatizovaný, spolehlivý a opakovatelný proces integrace, testování a nasazování softwaru, čímž urychluje vývoj, snižuje riziko chyb a

Pojem	Popis pojmu
	zvyšuje konzistenci produkčních nasazení.
CISA (Cybersecurity and Infrastructure Security Agency (USA)	CISA je vládní agentura USA, jejímž cílem je chránit kritickou infrastrukturu Spojených států před fyzickými i kybernetickými hrozbami, podporovat odolnost systémů, koordinovat reakce na incidentech a prohlubovat partnerství mezi státní správou, soukromým sektorem a dalšími partnery v oblasti bezpečnosti.
Cloning	Cloning znamená zhotovení plnohodnotné, identické kopie existujícího systému nebo jeho části, kterou lze využít samostatně k dalším účelům.
Cloud computing	"Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB) - služba informační společnosti, která umožňuje samoobslužnou správu a široký vzdálený přístup k rozšiřitelnému a pružnému seskupení sdílených výpočetních zdrojů, včetně těch rozmístěných na více místech Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS) - způsob zajištění provozu ISVS či jeho části prostřednictvím dálkového přístupu ke sdílenému technickému nebo programovému prostředku poskytovanému poskytovatelem cloud computingu"""
Cloud-native	Cloud-native znamená vytvářet a provozovat aplikace tak, aby byly nezávislé na konkrétní fyzické infrastruktuře, maximálně využívaly automatizaci, dynamické škálování, kontejnery, mikroslužby, DevOps, CI/CD, infrastructure as code a další moderní cloudové technologie. Tyto aplikace je možné rychle a efektivně vyvíjet, provozovat, nasazovat a

Pojem	Popis pojmu
	rozšiřovat v dynamicky se měnícím cloudovém prostředí.
Cloud-to-Cloud Backup	Cloud-to-Cloud Backup (C2C backup) je zálohovací postup, kdy jsou data uložená v jedné cloudové službě automaticky kopírována do jiné cloudové služby, a tím je zajištěna jejich ochrana i mimo původní platformu. Tento typ zálohy plní podobnou funkci jako tradiční „off-site“ záloha – chrání data před ztrátou, chybou, kybernetickým incidentem nebo selháním původní služby
Compliance	Compliance je schopnost a průběžná praxe organizace prokázat, že všechny její procesy, postupy, systémy a pracovníci odpovídají a dodržují platné zákony, oborové regulace, smluvní požadavky i vlastní interní pravidla.
Confidential Computing	Confidential Computing je technologie, která umožňuje ochranu dat v průběhu jejich zpracování (tedy „data in use“) prostřednictvím hardwarově chráněného a izolovaného prostředí, tzv. Trusted Execution Environment (TEE). Na rozdíl od běžného šifrování, které chrání data při přenosu („in transit“) nebo při uložení („at rest“), confidential computing přidává ochranu i v okamžiku, kdy jsou data aktivně zpracovávána v paměti.
Containerization	Kontejnerizace je způsob „balení“ a provozu aplikací, kdy jsou všechny závislosti aplikace uloženy do izolovaného kontejneru, což zajišťuje její přenositelnost, škálovatelnost i nezávislost na konkrétní infrastruktuře. Kontejnery urychlují vývoj, testování i nasazování moderních cloudových aplikací a jsou klíčovým prvkem cloud-native přístupu.
Context-aware access	Context-aware access je řízení přístupových práv, které rozhoduje na základě aktuální identity uživatele, stavu

Pojem	Popis pojmu
	zařízení, lokality, času a dalších kontextových parametrů, s cílem zajistit bezpečnější a flexibilnější přístup ke zdrojům a datům organizace.
CSA CoC (Cloud Security Alliance – Code of Conduct (GDPR))	CSA Code of Conduct (CoC) for GDPR Compliance je profesní standard vytvořený organizací Cloud Security Alliance, jehož cílem je pomoci poskytovatelům cloudových služeb (CSPs) a zákazníkům cloudu splnit požadavky evropského Obecného nařízení o ochraně osobních údajů (GDPR) a zvýšit transparentnost úrovně ochrany osobních dat v cloudových službách.
CSC (Cloud security compliance)	Cloud security compliance představuje soubor procesů, opatření a kontrol, které mají zajistit, že všechny cloudové služby a prostředí organizace odpovídají platným právním, regulatorním a oborovým požadavkům na bezpečnost a ochranu dat v cloudu
CSIRT (Computer Security Incident Response Team)	CSIRT (Computer Security Incident Response Team) je specializovaný tým odborníků, který se v rámci definovaného pole působnosti zabývá řešením, koordinací a prevencí bezpečnostních incidentů v počítačových sítích. Úkolem CSIRT je nejen reagovat na aktuální kybernetické hrozby a incidenty (např. útoky, úniky dat, zneužití služeb), ale také spolupracovat na jejich řešení — a to jak uvnitř organizace, tak napříč institucemi a často i mezinárodně
CSP (Cloud Service Provider)	CSP je firma, která poskytuje cloudové služby (infrastrukturu, platformu, software) prostřednictvím internetu, umožňuje škálování, platbu podle spotřeby a nabízí možnost rychle a efektivně využívat nejmodernější IT zdroje bez nutnosti budovat vlastní infrastrukturu

Pojem	Popis pojmu
CWPP (Cloud Workload Protection Platform)	CWPP je bezpečnostní platforma určená k ochraně všech typů workloadů (aplikací, kontejnerů, serverless funkcí, virtuálních i fyzických serverů) napříč cloudovými, hybridními i on-premise prostředími, poskytující průběžnou detekci hrozeb, správu zranitelností, compliance a centralizované řízení bezpečnosti
Data Guardian	Data Guardian je soubor bezpečnostních funkcí (nebo konkrétní role), který poskytuje kontextově řízenou ochranu, monitoring, řízení a audit citlivých dat v celé organizaci – napříč prostředími, zařízeními a cloudem. Umožňuje komplexní ochranu dat před únikem, zneužitím či incidenty při současném splnění compliance požadavků
Data sovereignty	Data sovereignty znamená, že data podléhají právu země, ve které jsou fyzicky uložena, a tudíž jsou přístupná, chráněná i kontrolovaná podle místních zákonů a autorit – bez ohledu na zemi původu či vlastnictví samotné organizace nebo poskytovatele IT služeb.
DDoS protection	DDoS protection je vícestupňový proces detekce, blokace a adaptivní obrany proti masivnímu distribuovanému zahlcení služby škodlivým provozem, realizovaný kombinací pokročilého monitoringu, filtrování, strojového učení a specializovaných bezpečnostních technologií, který zajišťuje dostupnost online služeb a chrání je před útoky typu Distributed Denial of Service
DevOps	DevOps je moderní metodika a soubor kulturních, organizačních, technických a procesních postupů, která propojuje a integruje vývoj softwaru (Development, zkr. „Dev“) s jeho správou a provozem (Operations, zkr. „Ops“). Cílem DevOps je umožnit rychlejší, spolehlivější a

Pojem	Popis pojmu
	kvalitnější vývoj, testování, nasazení a provozování aplikací díky úzké spolupráci týmů, vysoké míře automatizace a průběžnému zlepšování.
Disaster recovery	Disaster Recovery označuje souhrn opatření, plánů a technologií, které organizaci umožní co nejrychleji obnovit klíčové IT služby a data po katastrofě nebo vážném výpadku, čímž zajistí pokračování zásadních činností a minimalizuje ztráty. Je nedílnou součástí řízení kontinuity provozu (Business Continuity Management).
DLP (Data Loss Prevention)	DLP je soubor technologií, nástrojů, pravidel a procesů určených k ochraně citlivých dat před jejich neoprávněným přístupem, únikem, ztrátou či zneužitím. Cílem DLP je identifikovat, monitorovat a chránit data – ať už uložená (data at rest), přenášená (data in motion) nebo právě používaná (data in use) – a zabránit jejich úniku, například prostřednictvím e-mailů, cloudových úložišť, USB zařízení či tisku
DNS (Domain Name System)	DNS je systém, který umožňuje vyhledávat a spojovat doménová jména s příslušnými IP adresami, a tím usnadňuje používání internetu pro lidi i technologie.
DORA (Digital Operational Resilience Act) či DOA	DORA je zásadní evropské nařízení, které klade důraz na prevenci, monitoring a zvládání ICT rizik u všech relevantních hráčů finančního sektoru i jejich klíčových dodavatelů. Od 17. ledna 2025 budou muset jeho požadavky splňovat prakticky všechny významné finanční společnosti v EU a jejich dodavatelé ICT služeb – vše s cílem ochrany stability, bezpečnosti a důvěry v digitální finanční ekosystém
DPIA (Data Protection Impact Assessment)	DPIA neboli posouzení vlivu na ochranu osobních údajů je proces, kterým správce osobních údajů identifikuje,

Pojem	Popis pojmu
	vyhodnocuje a zvládá rizika, která dané zpracování osobních údajů představuje pro práva a svobody fyzických osob. DPIA je klíčovým nástrojem řízení rizik podle GDPR a jeho účelem je zajistit, že při plánovaném zpracování osobních údajů budou zohledněny a dostatečně chráněny základní práva subjektů údajů, zejména jejich právo na soukromí.
DRP (Disaster Recovery Plan)	Disaster Recovery Plan (DRP) je systematický, formálně zdokumentovaný soubor postupů, který stanovuje, jak organizace obnoví své klíčové IT systémy, data a kritické technologie po závažné havárii, kybernetickém útoku, přírodní katastrofě nebo jiné mimořádné události. Cílem DRP je minimalizovat dopady incidentů na provoz organizace, zkrátit dobu obnovy a zajistit pokračování činnosti s co nejmenším výpadkem.
Dynamické playbooks	Automatizované a adaptabilní scénáře reakce na bezpečnostní incidenty, které definují postupy krok za krokem v závislosti na typu a závažnosti incidentu. Umožňují rychlou, konzistentní a efektivní reakci na aktuální hrozby, často se integrují s nástroji pro automatizaci bezpečnostních operací (SOAR).
Edge computing	Edge computing je technologie, která umožňuje zpracovávat a analyzovat data přímo tam, kde vznikají, nikoli až v centrálních datových centrech. Minimalizuje tak potřebu přenosu velkých objemů dat, urychluje reakce systému a odlehčuje hlavní cloudové zdroje
Edge-to-Cloud Continuum	Edge-to-Cloud Continuum je spojitá, technicky i provozně integrovaná infrastruktura, která usnadňuje plynulý přesun, zpracování a analýzu dat napříč edge (periferními) zařízeními, lokalizovanými servery, uzly a

Pojem	Popis pojmu
	centrálními cloudovými platformami, v závislosti na požadavcích dané úlohy
EDPB (European Data Protection Board)	European Data Protection Board (EDPB) je nezávislý evropský orgán, který dohlíží na jednotné a konzistentní uplatňování pravidel ochrany osobních údajů v rámci celé Evropské unie (EU) i Evropského hospodářského prostoru (EHP). EDPB byla zřízena 25. května 2018 současně se vstupem v platnost Obecného nařízení o ochraně osobních údajů (GDPR) a nahradila předchozí pracovní skupinu WP29
Egress	Egress v IT a cloudových sítích označuje odchozí tok dat z určitého prostředí ven. V kontextu cloudových služeb se egress často zpoplatňuje („egress fees“) – poskytovatelé účtují paušál nebo cenu za gigabajt dat, která opouštějí jejich infrastrukturu.
Elasticity	Elasticita v cloudu umožňuje zákazníkům snadno škálovat využívání zdrojů nahoru nebo dolů podle měnících se potřeb. Elasticita je automatická a dynamická, přizpůsobující se aktuální poptávce
EMG2C (Explore–Make–Go-to-Cloud metodika - IT)	EMG2C je zkratka pro metodiku digitální nebo cloudové transformace v Itálii: Explore – Make – Go-to-Cloud. Slouží jako rámec pro systematický, fázový přechod informačních systémů, aplikací nebo procesů do cloudového prostředí.
Encryption at rest	Encryption at rest je šifrování dat během jejich uložení na fyzickém médiu s cílem znemožnit jejich zneužití při případném neautorizovaném přístupu k úložišti.
Encryption in transit	Encryption in transit je metoda, kdy jsou data při svém pohybu napříč sítí šifrována tak, aby byla čitelná pouze pro oprávněné příjemce, což chrání jejich důvěrnost a integritu před zachycením a zneužitím během přenosu

Pojem	Popis pojmu
ENISA (European Union Agency for Cybersecurity)	ENISA (European Union Agency for Cybersecurity) je agentura Evropské unie, jejímž hlavním úkolem je posilovat kybernetickou bezpečnost napříč Evropou a zajišťovat vysokou, společnou úroveň ochrany sítí, informací a digitální infrastruktury v celé EU. Byla zřízena v roce 2004 a sídlí v Aténách, s kancelářemi v Heraklionu a Bruselu
Ephemeral Token	Ephemeral token je krátkodobý autentizační/přístupový token, který platí jen po omezenou dobu, což výrazně zvyšuje bezpečnost a omezuje prostor pro zneužití citlivých údajů nebo služeb v případě jejich kompromitace.
EUCS (EU Cloud Services Scheme - certifikace ENISA)	EUCS je celoevropská certifikační schéma kybernetické bezpečnosti pro cloudové služby, které vzniklo pod záštitou agentury ENISA a vychází z požadavků nařízení EU o kybernetické bezpečnosti (Cybersecurity Act). Cílem EUCS je sjednotit a zvýšit úroveň kybernetické bezpečnosti cloudových služeb v rámci celé EU, podpořit digitální suverenitu a zjednodušit výběr bezpečných cloudových řešení pro zákazníky z veřejného i soukromého sektoru
Failover	Failover je mechanismus v oblasti informačních technologií a síťových služeb, jehož cílem je automatické nebo poloautomatické převedení provozu z primárního (hlavního) systému, serveru, sítě či aplikace na záložní (sekundární) systém v případě výpadku, selhání nebo zhoršení funkčnosti primárního prostředku. Cílem failoveru je minimalizovat dobu nedostupnosti služeb, zajistit jejich vysokou dostupnost a provozní kontinuitu i při chybách hardware, software nebo sítí.
Federated Identity	Federated identity je koncept řízení digitální identity, který umožňuje propojit

Pojem	Popis pojmu
	a sdílet uživatelovu elektronickou identitu napříč více vzájemně důvěřujícími, ale nezávislými identity management systémy a organizacemi. Uživatel tak může používat jeden soubor přihlašovacích údajů k bezpečnému a bezproblémovému přístupu k různým aplikacím, službám nebo doménám napříč partnery, aniž by se musel opakovaně přihlašovat a spravovat více účtů
Federation	Federation je propojení a důvěryhodná výměna identit a služeb mezi nezávislými institucemi, které uživatelům umožňuje pohodlný a bezpečný přístup ke sdíleným systémům pouze s jedním ověřením.
FinOps	FinOps je kultura a soubor procesů, které pomáhají firmám spravovat a optimalizovat náklady na cloud tak, aby maximalizovaly obchodní hodnotu svých cloudových investic prostřednictvím spolupráce různých týmů a datově řízených rozhodnutí.
Firewall	Firewall je zařízení nebo software, který chrání síť a informační systémy tím, že podle nastavených pravidel filtruje a řídí síťový provoz mezi důvěryhodnými a nedůvěryhodnými částmi prostředí.
Function as a Service (FaaS)	FaaS je cloudová služba, v rámci, které uživatel nasazuje a provozuje jednotlivé funkce (malé úseky aplikační logiky), jež se automaticky spouští v reakci na vybrané události, přičemž poskytovatel plně zajišťuje alokaci, škálování i správu výpočetních zdrojů. Uživatel platí jen za skutečně využitý výpočetní čas.
G-Cloud	G-Cloud je britská vládní iniciativa, jejímž cílem je usnadnit nákup cloudových služeb veřejným institucím ve Spojeném království. G-Cloud funguje jako rámcový procurement systém: poskytovatelé cloudových (hostingových, softwarových i

Pojem	Popis pojmu
	podpůrných) služeb se za předem definovaných podmínek zaregistrují a své služby nabídnou přes online katalog – tzv. Digital Marketplace
GDPR (General Data Protection Regulation)	GDPR (General Data Protection Regulation, Nařízení (EU) 2016/679) je evropské nařízení, které stanovuje komplexní právní rámec pro ochranu osobních údajů jednotlivců na území Evropské unie (EU) a Evropského hospodářského prostoru (EHP). Patří mezi nejpřísnější zákony na ochranu soukromí na světě a jeho vzorem se inspirují další země mimo EU
GDS (Government Digital Service - UK)	GDS je digitální centrum britské vlády a klíčová jednotka v rámci Department for Science, Innovation and Technology (DSIT). GDS určuje, vede a realizuje vizi moderní digitální vlády ve Spojeném království. Je odpovědný za strategii, standardy a klíčové digitální produkty i infrastrukturu napříč celým státním sektorem
Geo-redundancy	Geo-redundancy je postup, kdy jsou klíčová data a systémy provozovány a synchronizovány ve více oddělených geografických lokalitách, aby byla zajištěna jejich nepřetržitá dostupnost, rychlá obnova při haváriích a odolnost vůči výpadkům lokální infrastruktury
Geo-replication	Geo-replication je technologický mechanismus, který vytváří a udržuje synchronní nebo asynchronní kopie dat ve více geograficky oddělených lokalitách, a tím významně zvyšuje jejich dostupnost, bezpečnost a odolnost vůči výpadkům nebo katastrofám
Governance	Governance je rámec řízení a dozoru, který vymezuje, jak jsou organizace, procesy nebo technologie spravovány, jaká mají pravidla, kdo a za co zodpovídá, s cílem zajistit

Pojem	Popis pojmu
	transparentnost, soulad s předpisy, efektivitu a minimalizaci rizik.
Hot / Cold Stand-By	Hot Stand-By i Cold Stand-By jsou strategie zálohování a zotavení po havárii (disaster recovery), které určují, jak rychle a spolehlivě může organizace obnovit provoz při výpadku hlavního systému: Hot Stand-By = okamžitá, kontinuální záloha s minimální ztrátou času i dat, vhodná tam, kde i krátký výpadek znamená velké riziko. Cold Stand-By = záložní systém mimo provoz, zapínaný až v případě havárie; zahájení provozu trvá déle a může znamenat určitý úbytek dat
HSE (Health Service Executive - Irsko)	HSE je ústřední státní agentura a největší zaměstnavatel v irském zdravotnictví, která zajišťuje všechny veřejné zdravotní a sociální služby v Irsku. HSE je irskou obdobou britského NHS a řídí poskytování péče všem obyvatelům země – v nemocnicích, komunitách i v domácím prostředí.
HSM (Hardware Security Module)	HSM je fyzické, speciálně navržené zařízení, které zajišťuje bezpečnou generaci, správu, ukládání a používání kryptografických klíčů a provádění kryptografických operací (šifrování, dešifrování, digitální podepisování, autentizace) v chráněném prostředí. HSM je považován za pevný „root of trust“ (kořen důvěry) v bezpečnostní infrastruktuře.
Hybrid cloud	Hybridní cloud je kombinace veřejného a privátního cloudu (nebo místní infrastruktury), která umožňuje organizacím flexibilně spravovat a přesouvat aplikace a data mezi oběma prostředími s cílem optimalizovat výkon, náklady a zabezpečení podle konkrétních potřeb.

Pojem	Popis pojmu
Hyperscaler	Velký globální poskytovatel veřejného cloudu s masivně škálovatelnou infrastrukturou (např. AWS, Microsoft Azure, Google Cloud)
IAM (Identity and Access Management)	IAM je framework procesů, politik a technologií, který slouží k řízení digitálních identit a kontrole přístupu uživatelů či zařízení k systémům, aplikacím a datům v organizaci. Cílem IAM je zajistit, aby správné osoby (nebo entity) měly odpovídající, časově i rozsahově omezený přístup k požadovaným zdrojům, zatímco je zabráněno neoprávněnému přístupu a zneužití oprávnění
Identity vault	Trezor identit – Identity vault je zabezpečené, šifrované úložiště pro správu a ochranu digitálních identit, autentizačních informací a citlivých uživatelských údajů, přístupné jen autorizovaným uživatelům a chránící data před neoprávněným přístupem i kompromitací
IDS (Intrusion Detection System)	IDS je bezpečnostní systém, který automaticky sleduje a vyhodnocuje provoz v síti nebo na zařízení s cílem včas odhalit známky průniku, kybernetického útoku nebo porušení politik, a generuje upozornění bezpečnostním operátorům.
IISSP (Integrovaný informační systém Státní pokladny)	IISSP je český IS pro efektivní a centralizované řízení veřejných financí státu. Funguje jako hlavní technologický a informační nástroj Ministerstva financí ČR pro správu, kontrolu a sledování toku finančních prostředků ve veřejném sektoru.
Incident response	Incident response je strategický a procesně řízený soubor aktivit určených k detekci, zadržení, odstranění a obnově po kybernetickém incidentu s cílem minimalizovat jeho dopady na

Pojem	Popis pojmu
	chod organizace a zvýšit její odolnost vůči budoucím útokům
Infrastructure as a Service (IaaS)	IaaS poskytuje základní IT zdroje jako prosté výpočetní prostředky, které mohou být využity k virtualizaci infrastruktury nebo pro náročné projekty jako strojové učení, big data nebo hosting. Zákazník získává přístup k virtualizované infrastruktuře, ale nemusí investovat do vlastního hardwaru.
Infrastructure as Code (IaC)	Infrastructure as Code (IaC) je způsob, jakým je celá IT infrastruktura navrhována, spravována a nasazována prostřednictvím kódu nebo strojově čitelných konfiguračních souborů, což zajišťuje automatizaci, konzistenci, opakovatelnost, rychlost a vyšší bezpečnost v řízení IT prostředků.
Integrace threat-intelligence feeds	Propojení s externími a interními zdroji dat o aktuálních kybernetických hrozbách (hackerův software, aktivity, zranitelnosti, známé IOC – indicators of compromise). Tyto informace pomáhají systémům včas detekovat nové a cílené útoky a přizpůsobit reakci.
Interoperability	Interoperabilita je vlastnost systémů, která jim umožňuje vzájemně komunikovat, sdílet a smysluplně využívat data nebo služby napříč technologiemi, organizacemi i hranicemi, často díky dodržování společných standardů a protokolů
IPS (Intrusion Prevention System)	IPS je systém, který automaticky detekuje a blokuje síťové nebo systémové hrozby v reálném čase, čímž aktivně chrání IT infrastrukturu před průniky, útoky a zneužitím
ISAE 3000 (International Standard on Assurance Engagements 3000)	ISAE 3000 je mezinárodní standard vydaný International Auditing and Assurance Standards Board (IAASB) zaměřený na poskytování ujištění v oblastech mimo tradiční audit nebo přezkum historických finančních

Pojem	Popis pojmu
	informací. Používá se zejména při ověřovacích zakázkách zaměřených na nefinanční oblasti, jako jsou interní kontroly, dodržování předpisů, udržitelnost, informační bezpečnost, ochrana osobních údajů (např. GDPR) či společenská odpovědnost firem (ESG/CSR)
ISDS (Informační systém datových schránek)	ISDS je český informační systém veřejné správy zajišťující důvěryhodnou, bezpečnou a elektronickou výměnu dokumentů mezi orgány veřejné moci, fyzickými i právnickými osobami. Systém umožňuje nahrazení klasické papírové pošty elektronickou komunikací s právními účinky jako u listinných dokumentů. ISDS je zřízen na základě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, a dalších návazných předpisů (například vyhláška č. 194/2009 Sb.)
ISO 27001 (Řízení bezpečnosti informací - norma)	ISO/IEC 27001 je mezinárodní norma, která stanovuje požadavky na systém řízení bezpečnosti informací (ISMS), tedy na soubor pravidel, opatření a praxí, jejichž cílem je chránit informace organizace před riziky a hrozbami díky systematickému, dokumentovanému a neustále zlepšovanému přístupu k zabezpečení dat, procesů, osob a technologií. Mezinárodní standard ISO 22301 definuje požadavky na systém řízení kontinuity činností a je základním rámcem pro zavádění business continuity v organizacích
ISVS (Informační systém veřejné správy)	ISVS je v českém právním rámci termín označující informační systémy, které přímo slouží výkonu veřejné správy nebo plnění jiných funkcí státu a veřejnoprávních korporací. Vymezení ISVS je zakotveno v zákoně č.

Pojem	Popis pojmu
	365/2000 Sb., o informačních systémech veřejné správy.
ITZBund (Informationstechnikzentrum Bund - DE)	ITZBund je centrální IT organizace německé spolkové vlády. Slouží jako klíčový IT poskytovatel pro veškerou federální administrativu a zajišťuje podporu digitalizace veřejné správy napříč Německem
KEO4 (Ekonomický systém ALIS pro obce)	KEO4 je moderní modulární ekonomický a evidenční informační systém, navržený pro potřeby obcí, měst, škol a příspěvkových organizací. Systém vyvíjí a dodává společnost ALIS spol. s r.o., přičemž KEO4 patří mezi nejrozšířenější řešení pro veřejnou správu a samosprávu v ČR – využívá jej přes 4 000 organizací, z toho více než 2 700 obcí
Klasický outsourcing	Klasický outsourcing je předání specifických firemních činností externímu dodavateli, který poskytuje dedikované, na míru šité služby pro konkrétního zákazníka, často s vlastními zdroji a personálem přidělenými danému projektu. Na rozdíl od cloudu, kde jsou služby zpravidla poskytovány standardizovaně, jsou zdroje sdíleny více zákazníky najednou (multi-tenant), a charakteristická je vysoká flexibilita, samoobslužnost a platba dle skutečné spotřeby, zatímco u klasického outsourcingu bývají smluvní vztahy a řešení individuálně nastavené podle potřeb konkrétní firmy, včetně plně dedikované (vyhrazené) serverové infrastruktury pro daného zákazníka.
KMS (Key Management System)	KMS je specializovaný systém (on-premise nebo cloudový), který bezpečně generuje, uchovává, distribuuje a spravuje kryptografické klíče po celou jejich životnost, s cílem zajistit ochranu dat, souladu s předpisy a prevenci úniku nebo zneužití klíčů

Pojem	Popis pojmu
KOMBIT (Dánské konsorcium sdílených služeb pro obce)	KOMBIT je municipálně vlastněná nezisková společnost, která slouží jako hlavní IT konsorcium dánských obcí. Byla založena v roce 2009 a je stoprocentně vlastněná asociací dánských měst a obcí (Local Government Denmark – KL)
Latency	Latency je časové zpoždění mezi odesláním požadavku a získáním odpovědi (nebo dokončením přenosu dat) v rámci systémů, sítí či zařízení. Nižší latence znamená rychlejší reakce, což je zásadní pro aplikace citlivé na čas, jako je online hraní, videokonference, průmyslová automatizace nebo rychlé obchodování.
Legacy systems	Legacy system je starší (zastaralý) informační systém, hardware či software, který je sice technicky překonaný a již není výrobcem podporován, přesto dál zůstává v reálném provozu organizace z důvodu specifických potřeb, vysokých nákladů nebo rizik spojených s jeho náhradou
Lift-and-Shift	Lift-and-shift je metoda migrace, při níž jsou aplikace a data přesunuty do cloudu téměř beze změny – tedy tak, jak jsou bez úprav architektury., často jako úvodní krok před další optimalizací
Load balancing	Load balancing (česky vyvažování zátěže) je IT technika, která rozděluje aktuální zátěž (například síťový provoz, aplikační požadavky nebo výpočetní úlohy) mezi více zařízení, serverů nebo jiných zdrojů, aby bylo dosaženo optimálního využití zdrojů, vyšší dostupnosti služeb, minimalizace doby odezvy a zvýšení spolehlivosti provozu. Load balancing pomáhá předcházet přetížení jednotlivých komponent systému a umožňuje jeho efektivní škálování.

Pojem	Popis pojmu
Measured service	Measured service označuje automatické měření a monitorování využívání cloudových zdrojů s cílem zajistit transparentnost, účtování podle skutečné spotřeby a efektivní správu kapacit. Uživatel platí pouze za to, co reálně využije.
MFA (Multi-Factor Authentication)	MFA označuje bezpečnostní mechanismus, při kterém je k ověření identity uživatele zapotřebí úspěšně prokázat alespoň dvě (často tři a více) z odlišných kategorií ověřovacích faktorů. Cílem je výrazně snížit riziko neoprávněného přístupu – i v případě kompromitace jednoho faktoru (např. hesla) útočníkovi nestačí k získání přístupu k systému.
Micro-Segmentation	Micro-segmentation je bezpečnostní metoda, která rozděluje síť do malých izolovaných segmentů, k nimž aplikuje detailní přístupová pravidla, s cílem omezit laterální pohyb hrozeb v síti a zvýšit celkovou úroveň bezpečnosti organizace
Microservices	Microservices je architektonický styl, ve kterém je aplikace tvořena souborem malých, nezávislých a rozhraním jasně oddělených služeb, které společně plní komplexní funkce systému.
Mirroring	Mirroring je IT metoda, při které se v reálném čase udržuje přesná kopie dat nebo systému na jiném zařízení či místě, aby byla zajištěna vysoká dostupnost, rychlá obnova a ochrana před ztrátou dat.
MISP (Malware Information Sharing Platform)	MISP (Malware Information Sharing Platform, někdy také MISP Threat Sharing) je široce využívaná open source platforma pro sdílení, ukládání, správu a korelaci informací o kybernetických hrozbách (Cyber Threat Intelligence, CTI). Platforma je navržena tak, aby organizacím umožnila efektivně

Pojem	Popis pojmu
	a bezpečně sdílet technické i netechnické informace o incidentech, malware, phishingových kampaních, zranitelnostech, a dalších indikátorech kompromitace (IoC), a tím posilovala možnosti detekce a reakce na útoky.
Monitoring	Soustavné a systematické sledování a zaznamenávání činností, stavů a událostí v informačních systémech, sítích nebo jiných technických prostředcích, za účelem detekce anomálií, incidentů, ověření souladu s bezpečnostní politikou, prevenci a včasného odhalení bezpečnostních hrozeb či narušení.
Monolithic	Monolithic je softwarová architektura, kde je celá aplikace vyvíjena, provozována a nasazována jako jeden nedělitelný celek – bez dělení na oddělené, samostatně nasaditelné části.
MTBF (Mean Time Between Failures)	MTBF (Mean Time Between Failures) je statistická metrika spolehlivosti technických zařízení nebo systémů. Udává průměrnou dobu (obvykle v hodinách), která uplyne mezi dvěma po sobě jdoucími poruchami zařízení během jeho běžného provozu. MTBF je typicky používán pro hodnocení spolehlivosti elektroniky, strojních zařízení, serverů, disků, síťových prvků a dalších komponent.
MTBF (Mean Time Between Failures)	MTBF je ukazatel spolehlivosti vyjadřující průměrnou dobu mezi dvěma poruchami zařízení během provozu, přičemž vyšší hodnota MTBF znamená nižší pravděpodobnost poruchy a vyšší spolehlivost systému
MTTR (Mean Time To Recovery)	MTTR (Mean Time To Recovery) je ukazatel spolehlivosti a provozní efektivity, který vyjadřuje průměrnou dobu potřebnou k obnovení plné funkčnosti systému, služby nebo komponenty po výpadku, incidentu či poruše. MTTR zahrnuje celý proces od

Pojem	Popis pojmu
	detekce a nahlášení problému, přes diagnostiku příčiny, provedení oprav (nebo obnovy), až po ověření, že se systém vrátil do standardního provozu
MTTR (Mean Time To Recovery)	MTTR je průměrná doba, kterou potřebuje tým nebo organizace na kompletní detekci, opravu a obnovu funkčnosti systému po jeho poruše. Čím nižší je MTTR, tím rychleji se podaří obnovit provoz zařízení nebo služby po výpadku
Multi-Cloud	Multi-Cloud je cloudová strategie, kdy organizace současně využívá a spravuje služby a infrastrukturu od více různých poskytovatelů veřejného cloudu, aby získala vyšší flexibilitu, odolnost, kontrolu nad náklady a možnost využít nejvhodnější řešení pro každý konkrétní účel
Multi-tenantní	Multi-tenantní prostředí či architektura umožňuje, aby jedna instance aplikace, služby nebo cloud infrastruktury sloužila více nezávislým zákazníkům (tenantům), přičemž každý z nich má svá vlastní data, konfiguraci a logická pravidla, avšak infrastrukturu sdílí s ostatními
NCSC (National Cyber Security Centre - UK)	NCSC je ústřední britská státní autorita pro kybernetickou bezpečnost a reakce na incidenty. Poskytuje jednotný zdroj odborného vedení, hájí zájmy státu i občanů, podporuje kritickou infrastrukturu a funguje jako most mezi vládou, průmyslem a veřejností v oblasti kybernetické bezpečnosti
NIS2	NIS2 je směrnice Evropské unie, která stanovuje jednotný právní rámec pro kybernetickou bezpečnost a posiluje ochranu sítí a informačních systémů v EU. Tato směrnice je nástupcem původní směrnice NIS z roku 2016 a byla vyhlášena jako směrnice (EU) 2022/2555. NIS2 reaguje na rostoucí složitost a četnost kybernetických

Pojem	Popis pojmu
	hrozeb a digitální transformaci společnosti.
On-demand self-service	Samoobslužné získávání cloudových zdrojů Dle NIST: „Spotřebitel si může automaticky a jednostranně zřídit výpočetní prostředky (například serverový čas a síťové úložiště) podle potřeby, bez nutnosti lidské interakce s každým poskytovatelem služby“.
On-premise prostředí	On-premise prostředí je způsob zajištění provozu informačního systému, kdy jsou veškeré klíčové hardwarové i softwarové prostředky (datová centra, servery, úložiště, síťová infrastruktura a související SW) fyzicky umístěny a plně spravovány samotným provozovatelem (organizací), zpravidla v jejích vlastních prostorách nebo ve výhradně smluvně kontrolovaných prostorách (např. vlastní serverovna, uzavřená housingová služba).
OPEX (Operating Expenditure)	OPEX (provozní náklady) označuje veškeré běžné výdaje, které firma nebo organizace vynakládá na každodenní zajištění svého provozu. Jedná se o neinvestiční, opakující se a nezbytné náklady spojené s běžným chodem podnikání – například mzdy zaměstnanců, nájemné, energie, údržbu, marketing, služby třetích stran, kancelářské potřeby či platby za software a cloud, ale také například účetní, právní a licenční poplatky
Orchestration	Orchestration (orchestrace) je proces a technologie pro plně automatizovanou koordinaci, správu a spojování různorodých IT služeb, úloh a komponent do jednotně řízeného, efektivně fungujícího celku se záměrem zjednodušit, zrychlit a zefektivnit provoz složitých informačních systémů.

Pojem	Popis pojmu
Pay-As-You-Go	Pay-As-You-Go je princip účtování za cloudové (nebo jiné IT) služby podle skutečné spotřeby zdrojů – uživatel platí jen za to, co reálně využije, bez nutnosti předplacených balíčků či dlouhodobých závazků.
PCO (Pult centrální ochrany)	Pult centrální ochrany je dohledové centrum, které na dálku monitoruje a vyhodnocuje signály ze střežených objektů, zajišťuje rychlou reakci na incidenty a poskytuje klientům vyšší úroveň ochrany majetku i osob
Penetration testing	Penetration testing (penetrační testování, zkráceně pentest) je autorizované simulované kybernetické útoky na informační systém, síť, aplikaci či firemní infrastrukturu, jejichž cílem je odhalit a využít bezpečnostní zranitelnosti stejně, jako by to udělal reálný útočník. Tento proces provádějí školení experti (tzv. ethical hackers) s povolením a jasně daným rozsahem práce.
Platform as a Service (PaaS)	PaaS je cloudová služba, která zákazníkovi poskytuje kompletní platformu pro vývoj, provoz a správu vlastních aplikací, přičemž správu infrastruktury, operačních systémů, síťování, úložiště a často i vývojových nástrojů, middleware a databází zajišťuje poskytovatel. Zákazník se soustředí pouze na samotný aplikační kód a logiku.
Playbooks	Playbook v IT a kybernetické bezpečnosti je strukturovaný soubor návodů, postupů a pravidel, které stanovují konkrétní kroky pro zvládnutí určité situace, typicky incidentu nebo opakované operace. Playbook slouží jako podrobný „scénář“, který zajišťuje, že tým reaguje efektivně, konzistentně a v souladu s osvědčenými postupy a interními politikami.

Pojem	Popis pojmu
PNRR (Piano Nazionale di Ripresa e Resilienza - IT)	PNRR je klíčový strategický plán italské vlády, vytvořený pro využití prostředků z evropského fondu Next Generation EU jako reakce na ekonomické a sociální škody způsobené pandemií COVID-19. PNRR je oficiální italský název pro národní plán obnovy a odolnosti, který vznikl v rámci celoevropského programu Next Generation EU (NGEU) a jeho hlavního pilíře – Recovery and Resilience Facility (RRF). Každý členský stát Evropské unie má svůj vlastní národní plán tohoto typu (vždy s různým názvem dle dané země) a Itálie svůj plán označuje právě zkratkou PNRR.
Private cloud	Privátní cloud označuje cloudové výpočetní zdroje používané výhradně jednou organizací. Na rozdíl od veřejného cloudu jsou služby a infrastruktura privátního cloudu udržovány v privátní síti a hardware i software jsou vyhrazeny pouze jedné organizaci. Privátní cloud může být provozován buď ve vlastních prostorách (on-premises) nebo u externího poskytovatele.
Production environment	Production environment je označení pro živé, ostré provozní prostředí, ve kterém je finální, funkční verze softwarové aplikace, systému nebo webu nasazena a používána skutečnými koncovými uživateli. Právě zde se software začíná reálně využívat k zamýšleným úkolům, jako jsou zákaznické objednávky, interní workflow nebo provoz firemních systémů.
Provisioning	Provisioning je proces automatizovaného zřizování, nastavování a správy IT zdrojů nebo přístupů potřebných pro chod systémů, aplikací a uživatelů, obvykle podle šablon či požadavků na okamžitou dostupnost a efektivitu.

Pojem	Popis pojmu
PSN (Polo Strategico Nazionale - suverénní cloud IT)	PSN (Polo Strategico Nazionale) je vlajková iniciativa Itálie v oblasti „suverénního cloudu“, která byla vytvořena s cílem vybavit státní správu (PA) a klíčové veřejné instituce vysoce bezpečnou, moderní a spolehlivou cloudovou infrastrukturou. Projekt vzešel ze strategických priorit stanovených v rámci Strategie Cloud Italia a je úzce propojen se Strategickým plánem obnovy a odolnosti (PNRR).
Public cloud	Veřejný cloud je typ výpočetního prostředí, kde jsou zdroje nabízeny třetí stranou prostřednictvím internetu a sdíleny mezi více organizacemi a jednotlivci. Poskytovatelé veřejného cloudu spravují veškerou infrastrukturu včetně serverů, úložišť a aplikací. Zákazníci využívají model "pay-as-you-go", kde platí pouze za skutečně využité služby.
Rapid elasticity	Rapid elasticity je základní vlastnost cloud computingu, která označuje schopnost cloudové infrastruktury automaticky a velmi rychle (prakticky v reálném čase) navyšovat či snižovat množství přidělených výpočetních zdrojů (například výpočetní výkon, úložiště, šířka pásma) v návaznosti na aktuální potřebu nebo poptávku aplikace či uživatele. Dle NIST: "Kapacity mohou být škálovány (provisioned and released) v některých případech automaticky tak, aby rychle odpovídaly aktuální poptávce. Pro uživatele se zdá, že dostupná kapacita je neomezená a je možné ji kdykoliv získat v jakémkoli množství".
RBAC (Role-Based Access Control – řízení přístupu na základě rolí)	RBAC je přístupový model, který reguluje oprávnění uživatelů na základě jejich pracovních rolí v organizaci, což zvyšuje bezpečnost, efektivitu správy a snižuje riziko neoprávněného přístupu

Pojem	Popis pojmu
Redundancy	Redundancy je záměrné vytváření záloh a duplicitních komponent ve vašem IT, infrastruktuře či systémech za účelem ochrany před poruchou a zajištění nepřerušeného provozu i při výpadku klíčové části systému
Refactoring	Refactoring je úprava vnitřní struktury zdrojového kódu s cílem zlepšit jeho kvalitu, přehlednost a efektivitu, přičemž navenek zůstává funkčnost softwaru nezměněná
Replication	Replication je IT metoda, při které dochází k vytváření a synchronizaci více shodných kopií dat, systémů nebo zdrojů na různých místech s cílem zvýšit dostupnost, spolehlivost a výkon informačních systémů a ochránit je před ztrátou či výpadkem
Resource pooling	Resource pooling je způsob sdílení a dynamického přidělování IT zdrojů více uživatelům z jednoho společného fondu, což umožňuje efektivní využití kapacit, vyšší škálovatelnost a nákladovou efektivitu služeb v cloudu i v moderních IT systémech
Rollback	Rollback je standardní mechanismus pro odvolání a zrušení nechtěných či chybných změn a obnovení systému či databáze do předchozího bezpečného a konzistentního stavu
RPO (Recovery Point Objective)	RPO je klíčový pojem v oblasti řízení kontinuity provozu a disaster recovery (plánování obnovy po havárii). Vyjadřuje maximální přípustnou dobu (nebo rozsah dat), za kterou mohou být data ztracena v důsledku havárie – tj. jak starou zálohu je organizace schopna akceptovat bez závažného narušení podnikání.
RTO (Recovery Time Objective)	RTO (Recovery Time Objective) je klíčový parametr řízení kontinuity provozu a disaster recovery, který určuje

Pojem	Popis pojmu
	maximální přípustnou dobu, po kterou může být aplikace, systém, služba nebo infrastruktura mimo provoz po havárii, výpadku nebo jiném neočekávaném incidentu Tj. dobu od začátku výpadku do obnovení provozu.
Sandbox deployment analýza	Isolované testovací prostředí, kam je bezpečnostní incident (např. podezřelý soubor nebo aktivita) nasazen a analyzován bez ovlivnění produkčního prostředí. Umožňuje bezpečný průzkum a detekci škodlivého chování v kontrolovaném prostředí.
Scalability	Škálovatelnost je schopnost systému, sítě nebo procesu zvládnout zvýšené nebo snížené množství práce tím, že se úměrně přidávají či odebírají výpočetní, úložné, síťové nebo jiné zdroje, aniž by byla ovlivněna funkčnost, spolehlivost či kvalita poskytovaných služeb.
SCS (Sovereign Cloud Stack - DE)	Sovereign Cloud Stack (SCS) je otevřený evropský projekt, jehož cílem je umožnit digitální suverenitu v oblasti cloudových služeb vytvořením transparentního, interoperabilního a snadno přenositelně provozovatelného cloudového prostředí. SCS vzniká na půdě Německa, je financován Ministerstvem hospodářství a ochrany klimatu (BMWK) a je úzce propojen s projektem GAIA-X – celoevropskou iniciativou pro důvěryhodnou datovou infrastrukturu
SecNumCloud	SecNumCloud je francouzská bezpečnostní certifikace pro cloudové služby, vydávaná národní agenturou ANSSI (Agence nationale de la sécurité des systèmes d'information). Je považována za nejvyšší standard pro bezpečnost a suverenitu cloudu ve Francii a slouží zejména státní správě, kritickým sektorům a všem organizacím, které požadují maximální ochranu a kontrolu nad svými daty.

Pojem	Popis pojmu
Serverless computing	Serverless computing je způsob poskytování cloudových služeb, při kterém uživatel neřeší správu, údržbu ani škálování serverové infrastruktury. Veškeré tyto technické detaily zajišťuje poskytovatel cloudu automaticky a „na pozadí“. Uživatel pouze vyvíjí a nasazuje vlastní aplikační kód, který se spustí v reakci na konkrétní události (např. HTTP požadavek, časovač, změna souboru).
Service Mesh	Service mesh je infrastruktura, která poskytuje transparentní, centralizovanou správu a monitoring komunikace mezi mikroslužbami, s důrazem na bezpečnost, škálovatelnost, spolehlivost a snadnou provozní kontrolu, a to prostřednictvím sítě proxy agentů a řídicí vrstvy spravující jejich chování.
Shared Responsibility Model	Shared Responsibility Model je rámec, který v prostředí cloudu přesně definuje, za které oblasti bezpečnosti, správy a provozu odpovídá poskytovatel služby a které musí řešit zákazník. Díky tomu se předchází nepokrytým rizikům, zvyšuje transparentnost a posiluje celková bezpečnost při využívání cloudových technologií
SIEM (Security Information & Event Management)	SIEM je technologie a koncept, který slouží k centrálnímu sběru, korelaci, analýze a vizualizaci bezpečnostních událostí a informací napříč IT infrastrukturou organizace. SIEM řešení jsou klíčovým nástrojem moderních bezpečnostních týmů (SOC – Security Operations Center) pro včasné odhalení hrozeb, účinnou reakci na incidenty a plnění požadavků na audit či compliance.
SLA (Service Level Agreement)	SLA je závazná dohoda mezi poskytovatelem a uživatelem služby, která stanovuje úroveň, způsob měření,

Pojem	Popis pojmu
	monitoring a sankce týkající se kvality a dostupnosti poskytovaných služeb
Snapshot	Snapshot je okamžitá kopie stavu dat nebo systému v určitém čase, kterou lze použít pro rychlou obnovu nebo návrat při chybě, havárii nebo nežádoucí změně.
SOAR (Security Orchestration, Automation and Response)	SOAR je technologie, která organizacím umožňuje automatizovat, integrovat a řídit bezpečnostní procesy a odezvy na incidenty s cílem zrychlit obranu, zvýšit efektivitu týmu a minimalizovat dopady kybernetických hrozeb.
SOC (Security Operations Center)	SOC je specializované centrum nebo tým, který permanentně sleduje, analyzuje a chrání IT systémy organizace před kybernetickými hrozbami, rychle detekuje a řeší bezpečnostní incidenty a zajišťuje celkovou kybernetickou bezpečnost organizace
SOC 2 (System and Organization Controls 2)	SOC 2 je mezinárodní rámec a auditní standard, který byl vyvinut Americkým institutem certifikovaných veřejných účetních (AICPA) pro hodnocení toho, jak organizace – zejména poskytovatelé cloudových a IT služeb – spravují a chrání data svých zákazníků
Sovereign Cloud	Sovereign Cloud je cloudové prostředí navržené tak, aby plně vyhovovalo požadavkům na datovou a digitální suverenitu – tedy aby veškerá data, aplikace a systémy byly provozovány, ukládány a chráněny výhradně v souladu s právním a institucionálním rámcem daného státu nebo regionu, bez rizika zahraničního zásahu či nedodržení lokálních předpisů.
SPCSS (Státní pokladna – Centrum sdílených služeb)	SPCSS je státní podnik zřízený Ministerstvem financí ČR. Je klíčovým poskytovatelem IT infrastrukturních a cloudových služeb pro státní správu a veřejný sektor v České republice

Pojem	Popis pojmu
	(eGovernment Cloud České republiky (eGC), je klíčová platforma pro provozování IT infrastruktury a služeb veřejné správy)..
SQL (Structured Query Language)	SQL je speciálně navržený jazyk pro práci s daty uloženými v relačních databázích. SQL umožňuje vytváření, modifikaci, správu a dotazování databázových tabulek s pomocí jasně definovaných příkazů. Patří mezi naprosto základní dovednosti pro práci s databázemi v IT, vývoji aplikací, analytice i správě dat.
Staging environment	Staging environment je preprodukční (testovací) IT prostředí s téměř shodnými parametry jako produkce, které umožňuje bezpečně ověřit připravenost nových verzí systému, změn a integrací před jejich ostrým nasazením.
Synchronization	Synchronizace je proces, při němž jsou víceprvkové nebo víceprocesové systémy uváděny do konzistentního, sladěného stavu – ať už jde o data, časy, procesy nebo stavy jednotlivých částí systému, a to kvůli zajištění správného a předvídatelného fungování v IT či jiných technologických oblastech
Tenant	Tenant je samostatná, logicky izolovaná skupina uživatelů či organizace v rámci sdílené cloudové nebo softwarové platformy, která má vlastní data a konfigurace, přestože sdílí infrastrukturu s ostatními tenanty systému.
Threat hunting	Threat hunting je proaktivní, lidsky vedený proces cíleného vyhledávání (a následné eliminace) skrytých, neznámých či pokročilých hrozeb v IT prostředí organizace, které unikly běžným detekčním technologiím. Hlavními nástroji jsou hluboká znalost prostředí, práce s daty, behaviorální analýza a threat intelligence

Pojem	Popis pojmu
Threat intelligence	Threat intelligence je proces a sada znalostí, které vznikají sběrem, analyzováním a distribuováním informací o kybernetických hrozbách, s cílem umožnit organizacím reagovat na útoky proaktivně, efektivněji řídit bezpečnost a chránit svá aktiva před aktuálními i budoucími riziky
Throughput	Throughput je technická metrika vyjadřující množství dat nebo operací, které je systém či síť schopna přenést nebo obsloužit za jednu sekundu či jinou jednotku času; je ukazatelem výkonnosti a kapacity daného řešení.
Total Cost of Ownership (TCO)	Total Cost of Ownership (TCO) neboli celkové náklady vlastnictví je ekonomická metoda nebo ukazatel, který vyjadřuje úplné náklady spojené s pořízením, provozem, údržbou, rozvojem a ukončením produktu, služby nebo investice v průběhu její životnosti. TCO zahrnuje nejen vlastní pořizovací cenu (investici), ale i všechny další výdaje vázané na vlastnictví nebo užívání – například servisní smlouvy, spotřebované energie, náklady na školení a lidské zdroje, provozní i režijní náklady, údržbu, upgrady, odstávky či likvidaci
Uptime	Uptime je technická metrika vyjadřující dobu, po kterou je systém či služba nepřetržitě dostupná a funkční bez výpadků, často uváděná v procentech za určité období.
Vendor Lock-In	Vendor lock-in znamená závislost zákazníka na jediném dodavateli, která mu znemožňuje nebo zásadně komplikuje přechod k jiné alternativě z technických, ekonomických nebo smluvních důvodů, což má negativní dopad na konkurenci, kvalitu i ceny služeb.

Pojem	Popis pojmu
Versioning	Versioning je systematická správa a označování změn softwaru, dokumentů, dat nebo rozhraní, která umožňuje jasně sledovat, identifikovat, vracet a koordinovat různé verze a vývojové větve v čase.
VPN (Virtual Private Network)	VPN je technologie pro bezpečné, šifrované propojení zařízení přes nedůvěryhodné sítě, která zajišťuje důvěrnost, integritu, anonymitu a umožňuje přístup do privátních sítí odkudkoliv
WAF (Web Application Firewall)	WAF je firewall navržený pro ochranu webových aplikací před útoky, které cílí na aplikační vrstvu, a zajišťuje filtraci, monitoring a blokování škodlivého webového provozu dle předdefinovaných či dynamicky aktualizovaných bezpečnostních pravidel, čímž chrání jak aplikace, tak jejich uživatele před širokou škálou hrozeb
Workload	Workload v informatice označuje výpočetní úlohu, proces nebo sadu úloh, které využívají konkrétní množství výpočetních, paměťových, úložných a síťových zdrojů za účelem provedení určitého zadání či operace. Workloadem může být jednorázový výpočet, běh aplikace, databázový dotaz, dávkové zpracování dat, provoz mikroslužby nebo správa celého ekosystému propojených aplikací.
X-Road	X-Road je open-source softwarová platforma určená pro bezpečnou, jednotnou a interoperabilní výměnu dat mezi organizacemi v rámci komplexních ekosystémů. X-Road slouží zejména jako páteřní infrastruktura e-governmentu a digitálních služeb v řadě zemí, například v Estonsku a Finsku.
Zero Trust	Zero Trust (model nulové důvěryhodnosti) je bezpečnostní

Pojem	Popis pojmu
	strategie, která nikdy automaticky nevěří žádnému uživateli, zařízení či aplikaci – každý přístup musí být opakovaně a důsledně ověřován a autorizován na základě aktuálního kontextu, a to bez ohledu na umístění v síti; cílem je minimalizace rizika v moderním, dynamickém IT prostředí.
ZoISVS	Zákon o informačních systémech VS (365/2000 Sb.), zákon, který je klíčovou legislativní normou České republiky pro oblast řízení, správy a bezpečnosti veškerých informačních systémů provozovaných veřejnou správou
ZoKB	Zákon o kybernetické bezpečnosti č.181/2014 Sb. a jeho novela č. 264/2025 Sb., která vstoupí v účinnost 1. listopadu 2025 V obou případech je to hlavní český zákon určující povinnosti a pravidla v oblasti kybernetické bezpečnosti, jehož cílem je chránit kritické systémy, data a sítě v ČR a sladit požadavky kybernetické ochrany s evropskou legislativou.

4.2.1 Internetové zdroje

1. https://xpert.digital/en/multi-cloud-strategy/
2. https://newsroom.orange.com/capgemini-and-orange-announce-plan-to-create-bleu-a-company-to-provide-a-cloud-de-confiance-in-france/
3. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/05/digital-government-review-of-sweden_7917ba3f/4daf932b-en.pdf
4. https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Denmark_vFinal_0.pdf
5. https://en.digst.dk/digital-governance/new-technologies/guide-on-the-use-of-cloud-services/
6. https://leadiq.com/c/kombit-as/5a1d8933240000240062b0b7
7. https://systematic.com/int/industries/library-learning/news-knowledge/news/systematic-re-wins-valuable-contract-for-denmark-s-library-system/
8. https://www.bus-ex.com/article/kombit
9. https://offentligsektorsdataforum.wordpress.com/wp-content/uploads/2015/12/9-3-kommunernes-it-fc3a6llesskab-kombit.pdf
10. https://www.riigipilv.ee
11. https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Estonia_vFinal.pdf
12. www.rit.ee/en/news/estonian-public-sector-opens-door-public-cloud-services
13. https://e-estonia.com/solutions/e-governance/government-cloud/
14. Radar, "Digital Government Efficiency Report", 2021 (dostupné na https://radar.se/digital-government-efficiency)
15. Copenhagen Economics, "Public Sector Cloud Savings", 2022 (https://copenhageneconomics.com/public-sector-cloud-savings)
16. Estonská vláda, "Digital Estonia 2024", 2024 (https://riigikantselei.ee/digital-estonia-2024)
17. https://aws.amazon.com/compliance/bsi-c5/
18. https://38northsecurity.com/security-compliance/global/french-secnumcloud/
19. https://www.ssi.gouv.fr/administration/guide/secnumnud-cloud-referentiel-de-certification-pour-les-services-de-confiance-en-cloud/
20. https://digital-strategy.ec.europa.eu/en/policies/cloud-computing
21. https://digital-strategy.ec.europa.eu/en/policies/simpl
22. WIK-Diskussionsbeitrag Nr. 529 „Cloud-Lösungen für die öffentliche Verwaltung“ (12/2024) (https://awsdigitaldecade.publicfirst.co.uk/germany/?lang=de)
23. Lünendonk-studie „Cloud-Transformation im öffentlichen Sektor“ (04/2025), kap. „Cloud-Kostenmanagement“ (https://www.datagroup.de/wp-content/uploads/2021/08/LUE_IT_Studie-2021_DATAGROUP.pdf)
24. ZNT Quadriga-Studie „Fair Software Licensing & Cloud in öffentlichen Unternehmen“ (02/2025) (https://themunicheye.com/Public-Sector-Cloud-Transition-Could-Cost-Up-to-EUR120-Million-11298)
25. https://www.steel-eye.com/news/data-ownership-the-end-of-extraction-fees-eu-data-act-mandates-freedom-for-your-archives-part-2
26. https://www.fivetran.com/blog/know-your-rights-you-can-control-extract-and-move-your-data
27. EY Rapport « Moderniser l’État par le numérique » (2024) (https://digitales.hessen.de/sites/digitales.hessen.de/files/2022-04/nachhaltigkeitsstudie.pdf)
28. https://www.trade.gov/market-intelligence/italy-information-technology-national-strategic-hub-cloud-services
29. https://lucianocastro.com/en/national-strategic-pole-10-answers-on-psn/

30. https://www.agid.gov.it/en/news/agid-joins-polo-strategico-nazionale-further-step-cloud-italia-strategy
31. https://www.italiadomani.gov.it/en/Interventi/investimenti/infrastrutture-digitali.html
32. https://www.polostrategiconazionale.it/media/news/psn-integra-il-listino-servizi-2025-nuove-soluzioni-innovative-per-la-digitalizzazione-delle-pa-psn/
33. AWS Public Sector Blog, 2022 (https://aws.amazon.com/blogs/publicsector/the-impact-of-the-cloud-on-the-public-administration-in-italy/)
34. Transforming Government Data Centres“ (Cabinet Office, 2018) – https://www.gov.uk/government/publications/transforming-government-data-centres
35. The UK Government Cloud Strategy“ (GDS, 2014) (https://digital.blog.gov.uk/2014/07/10/uk-government-cloud-strategy/)
36. Crown Hosting Data Centres – Strategic Overview“ (Ark Data Centres, 2020) – https://arkdatacentres.co.uk/crown-hosting/
37. https://digitalnicesko.gov.cz/media/files/Informa%C4%8Dn%C3%AD_koncepce_%C4%8Cesk%C3%A9_republiky_2024.docx.pdf
38. https://www.businessinfo.cz/clanky/ceska-republika-si-polepsila-v-oblasti-digitalizace-sluzeb-verejne-spravy-zustava-ale-v-dolni-polovine-evropskeho-zebricku-desi/
39. https://blog.cesko.digital/2024/10/priciny-problemu-digitalizace-verejne-spravy-v-cr
40. https://www.czechbusinessguide.com/content-of-book-research-and-development-digital-and-innovation/
41. https://www.mt-legal.com/pravidla-pro-vyuzivani-cloud-computingu-organy-verejne-spravy-z-pohledu-zzvz/
42. https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/
43. https://techcrunch.com/2025/02/26/microsoft-finalizes-its-eu-sovereign-cloud-project/
44. https://cpl.thalesgroup.com/blog/encryption/thales-digital-security-google-next-2025
45. https://www.s3ns.io/en
46. https://www.leaseweb.com/en/about-us/sovereignty
47. https://www.heise.de/en/news/Delos-Sovereign-cloud-10-to-20-more-expensive-than-Microsoft-s-public-cloud-10102043.html
48. https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/
49. https://opensourcelab.dfki.de/the-cyber-state-opens-the-worlds-first-cyber-embassy/
50. https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/
51. https://focus.namirial.it/psn-polo-strategico-nazionale-cose-come-funziona-2/
52. https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/
53. https://www.wired.it/cloud-polo-strategico-nazionale-servizi-microsoft-google-oracle-bandi-gare/
54. https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/
55. https://docs.italia.it/media/pdf/italian-cloud-strategy-docs/stabile/italian-cloud-strategy-docs.pdf
56. https://en.digst.dk/media/mndfou2j/national-strategy-for-digitalisation-together-in-the-digital-development.pdf
57. https://e-estonia.com/estonia-100-digital-government-services/
58. https://www.pwc.de/en/digitale-transformation/bsi-c5-german-bsi-catalogue-of-requirements-for-more-transparency-in-the-cloud.html
59. https://www.wanclouds.net/blog/migration-as-a-service/the-hidden-costs-of-on-prem-to-cloud-migration
60. https://www.wipro.com/applications/calculate-the-tco-savings-of-moving-to-oracle-cloud-infrastructure/

61. https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/metodiky-navody-formulare/metodika-tco-metodika-pro-vypocet-celkovych-nakladu-vlastnictvi-isvs
62. https://www.consilium.europa.eu/en/policies/top-cyber-threats/
63. https://lucysecurity.com/on-premise-vs-cloud-choosing-a-security-platform/
64. https://www.deloitte.com/us/en/insights/topics/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html
65. https://www.ospi.es/export/sites/ospi/documents/documentos/ENISA_Security-Framework-for-Governmental-Clouds.pdf
66. https://www.amchameu.eu/system/files/position_papers/eu_guidelines_public_procurement_cloud_services_final.pdf
67. https://ecipe.org/publications/boosting-efficiency-and-quality-in-eu-public-services-egovernment/
68. https://archi.gov.cz/_media/dokumenty:metodika_tco_ict_sluzeb_vs.pdf
69. https://www.cybersecurity.cz/data/eGovCloud.pdf
70. https://www.epenize.eu/cloudove-reseni-versus-on-premise/
71. https://www.prehleddotaci.cz/operacni-program/digitalni-podnik
72. https://www.businesswatchgroup.co.uk/why-cloud-based-security-is-safer-than-on-premise-in-2025/
73. https://www.milestonesys.com/resources/content/articles/cloud-based-surveillance-security/
74. https://archi.gov.cz/uvod_klicove_oblasti#cloud
75. https://www.cloudzero.com/blog/cloud-computing-statistics/
76. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/06/oecd-reviews-of-digital-transformation-going-digital-in-sweden_g1g904ac/9789264302259-en.pdf
77. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-hybrid-cloud/hybrid-cloud-security-best-practices/
78. https://cloudsecurityalliance.org/articles/hybrid-cloud-security-top-challenges-and-best-practices/
79. https://www.cloud4c.com/blogs/10-best-practices-for-effective-hybrid-cloud-governance
80. https://www.reco.ai/learn/hybrid-cloud-security
81. https://advanta.de/bsi-c5-audit/
82. https://www.gov.uk/guidance/government-cloud-first-policy
83. https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector
84. https://www.gov.uk/government/groups/public-services-network
85. https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector
86. https://digital-strategy.ec.europa.eu/cs/policies/cloud-computing
87. https://digital-strategy.ec.europa.eu/cs/library/study-cloud-security-healthcare-services
88. https://digital-strategy.ec.europa.eu/cs/policies/nis2-directive
89. https://www.europarl.europa.eu/news/sk/press-room/20160701IPR34481/kyberneticka-bezpecnost-nove-pravidla-na-zvysenie-odolnosti-voci-online-hrozbam
90. https://www.deloitte.com/cz-sk/cs/services/consulting/services/network-and-information-security-2-nis2-and-deloitte-nis2-maturity-assessment-tool.html
91. https://www.lupa.cz/clanky/regulace-podle-nis2-sluzba-cloud-computingu-nema-v-zakone-jasnou-definici/
92. https://cloudsecurityalliance.org/gdpr/eu-cloud-code-of-conduct
93. https://www.cloudcomputing-news.net/news/eu-body-to-investigate-public-sector-usage-of-cloud-services/

94. https://www.european-multicloud.eu/why-multi-cloud-is-the-go-to-strategy-for-european-businesses-in-2025/
95. https://www.rackwareinc.com/digital-operational-resilience-act-dora-and-the-need-for-multi-cloud-architectures
96. https://blog.equinix.com/blog/2024/06/06/how-the-european-data-act-could-impact-your-multicloud-strategy/
97. https://cispe.cloud/gaia-x-builds-momentum-with-first-federated-cloud-services-catalogue/
98. https://www.nonhuman.id/resources/federated-cloud-security
99. https://sprinto.com/blog/cloud-incident-response/
100. https://www.darktrace.com/cyber-ai-glossary/cloud-backup-and-disaster-recovery
101. https://www.euronews.com/my-europe/2025/02/20/cybersecurity-which-are-europes-most-vulnerable-countries
102. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
103. https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf
104. https://silicon-saxony.de/en/ibm-x-force-report-europe-recorded-the-most-cyberattacks-worldwide-in-2023/
105. https://cepa.org/article/unlock-data-flows-within-europe/
106. https://cepa.org/article/unlock-data-flows-within-europe/
107. https://itif.org/publications/2025/05/25/eu-cloud-service-restrictions/
108. https://www.elevityit.com/blog/cost-to-recover-from-a-cyberattack
109. https://www.barclaysimpson.com/how-much-does-it-cost-to-recover-from-a-cyber-security-breach/
110. https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/
111. https://www.straitstimes.com/world/europe/dutch-university-gets-cyber-ransom-money-taken-in-2019-back…-with-interest
112. https://www.cm-alliance.com/cybersecurity-blog/november-2023-biggest-cyber-attacks-data-breaches-ransomware-attacks
113. https://archi.gov.cz/nap:egovernment_cloud
114. https://www.egovernment.cz/inpage/cloud/
115. https://www.helios.eu/novinky/cloudove-reseni-je-vhodne-pro-organizace-a-subjekty-verejne-spravy
116. https://mv.gov.cz/soubor/klodwig-jakub-kyberneticka-bezpecnost-a-cloud-computing-pdf.aspx
117. https://www.promestaobce.cz/pravo/pracujete-v-cloudu-pozor-na-paragrafy/
118. https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce_dokldn_poadavk_pro_zpis_sluby_cloud_computingu-v.1.2.pdf
119. https://it.cz/servery-a-zalohovani/servery/2-cpu-servery
120. https://www.prolicence.cz/microsoft-windows-server/
121. https://www.abacus.cz/doem-windows-server-essentials-2025-64bit-1pk-1cpu-10core-pouze-k-serverum-abacus_d5108320.html
122. https://www.prolicence.cz/microsoft-windows-server/
123. https://greencloudvps.com/budget-windows-vps.php
124. https://www.vps-mart.com/ram/8gb
125. https://cloudzy.com/windows-2025-vps/

4.2.2 Další informace

/ Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen “ZoISVS”)

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 12/2020 Sb., o právu na digitální služby
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek (ZZVZ)
- Prováděcí vyhlášky a metodiky:
  - Vyhláška č. 315/2021 Sb. - stanovuje bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci podle zákona o kybernetické bezpečnosti.
  - Vyhláška č. 316/2021 Sb. - upravuje požadavky pro zápis do katalogu cloud computingu, včetně certifikací, auditů, penetračních testů a plánů kontinuity provozu.
  - Vyhláška č. 190/2023 Sb. - stanovuje bezpečnostní pravidla pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.
- Praktická pravidla a postupy (zjednodušeně):
  - Služby cloud computingu mohou OVS pro svoje ISVS využívat jen od poskytovatelů zapsaných v katalogu cloud computingu vedeném DIA. Zápis poskytovatele a zápis jeho nabídky cloud computingu potvrzuje, že poskytovatel splňuje definované požadavky na bezpečnost, důvěrnost, integritu a dostupnost dat (podrobnosti viz ZoISVS).
  - Úřady smějí pro svoje ISVS využívat pouze cloud computing, který byl zapsán do katalogu cloud computingu v bezpečnostní úrovni stejné nebo vyšší, než do které byl zařazen příslušný ISVS (nebo jeho část).

5. SEZNAM TABULEK