Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j.: 2009/2024-NÚKIB-E/630 • BRNO • 15. BŘEZNA 2024

STRATEGICKÁ ANALÝZA

CLOUDY UMOŽNUJÍ SNÍŽENÍ NÁKLADŮ A SNADNÝ VZDÁLENÝ PŘÍSTUP, AVŠAK DOCHÁZÍ KE ZTRÁTĚ PLNÉ KONTROLY NAD DATY

SHRNUTÍ

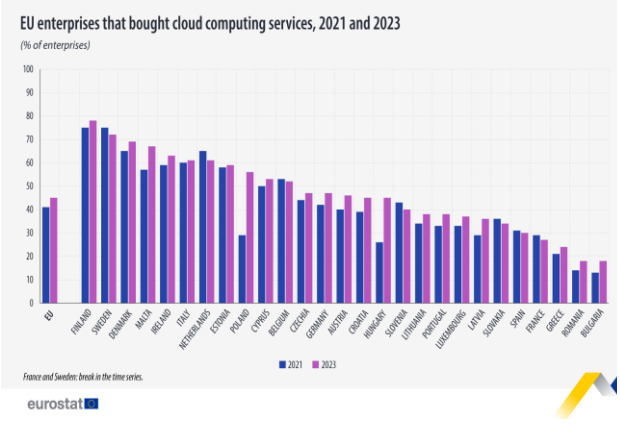
- **Cloudovými službami se rozumí služby umožňující vzdálený samoobslužný přístup k výpočetním zdrojům, které jsou zpravidla schopné se přizpůsobit potřebám zákazníků. Velké množství firem i státních institucí po celém světě využívá cloudových služeb.**
- **Ukládat data a využívat další cloudové služby v infrastruktuře poskytovatele přináší pro uživatele bezpečnostní výzvy. Při využívání cloudových služeb nevyhnutelně dochází k předávání velké části kontroly nad daty poskytovateli, proto je klíčová jeho důvěryhodnost. V konečném důsledku je totiž vždy prakticky odpovědný zákazník – uživatel, který by si měl být naprosto jistý důvěryhodností poskytovatele.**
- **Při posuzování dodavatele je tedy zásadní brát v potaz i to, v jakém státě společnost sídlí a kde budou data fyzicky ukládána. Pro poskytovatele nebo fyzické uložiště může platit právní rámec jiných zemí, které mohou mít možnost si na jeho základě vynutit přístup k datům.**
- **V současné době jsou již cloudové služby v ČR hojně využívány, a to jak soukromými subjekty, tak orgány veřejné moci.**
- **Regulací cloudových služeb ve státní správě se NÚKIB intenzivně zabývá. Neregulované a soukromé subjekty by samy měly dodržovat zásady bezpečného užívání cloudů, jako prověření důvěryhodnosti dodavatele, právních rámců, ve kterých se pohybuje, a zvážení, jaká data ukládat na cloud s ohledem na jejich citlivost.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

PANDEMIE AKCELEROVALA PŘECHOD NA CLOUDOVÉ SLUŽBY

Cloud computing je služba, která umožňuje vzdálený samoobslužný přístup k výpočetním zdrojům, jež jsou zpravidla schopné se přizpůsobit potřebám zákazníků. Takovými výpočetními zdroji jsou zejména sítě, servery či jiná infrastruktura, operační systémy, software, úložiště, aplikace a služby. Cloudové služby tak umožňují ukládat data a užívat další služby přes internet ve vzdáleném systému, který je spravován třetí stranou. Data tedy nejsou uložena na fyzickém „domácím“ úložišti (typicky na pevném disku), ale uživatel je svěřuje do správy externího poskytovatele cloudové služby, který data shromažďuje na vzdálených serverech po celém světě.

Obrázek 1: Srovnání využívání cloudových služeb v EU mezi lety 2021 a 2023 (větší rozlišení)



Zdroj: ec.europa.eu

Pandemie viru covid-19 přinutila firmy rychle se přeorientovat na režim home-office a zajistit spolehlivý vzdálený přístup k datům pro všechny zaměstnance, přičemž investice do cloudových služeb se ukázaly být vhodným prostředkem, jak těchto cílů dosáhnout. Poskytovatelé cloudových služeb se navíc během pandemie osvědčili a dokázali ustát vysoký nárůst poptávky, čímž jejich kredibilita ještě vzrostla.[1]

Existují stovky různých systémů cloudových produktů, přibližně rozdělitelných do několika kategorií, které nabízejí širokou škálu služeb, od klasických osobních úložišť pro ukládání nebo zálohování soukromých souborů konkrétního uživatele až po pokročilé databázové služby či nástroje umělé inteligence (viz Příloha 1).

Cloudové služby nabízejí oproti klasickým řešením přístup z jakéhokoliv zařízení s podporou internetu. Data jsou tedy dostupná kdykoliv a odkudkoliv a uživatel není vázán na přístup např. jen ze svého osobního počítače. K datům se navíc online dostane každý, kdo k tomu má povolení. Pokud to nastavení zvolené vlastníkem umožnuje, další uživatelé mohou data libovolně upravovat a sdílet v reálném čase. **Cloudové služby jsou využívány i jako spolehlivá záloha dat pro případ selhání domácího úložiště nebo nedostupnosti dat v důsledku kybernetického útoku.**

BOX 1: Modely cloudových služeb

Veřejný – sdílí data a nabízí služby široké veřejnosti se stejnou nebo velmi podobnou funkcionalitou pro všechny klienty (např. Amazon Web Services, Microsoft Azure, Google Cloud Platform).

Privátní – nabízí služby přes privátní interní síť; cloud je provozován pouze pro organizaci, a to buď organizací samotnou nebo třetí stranou.

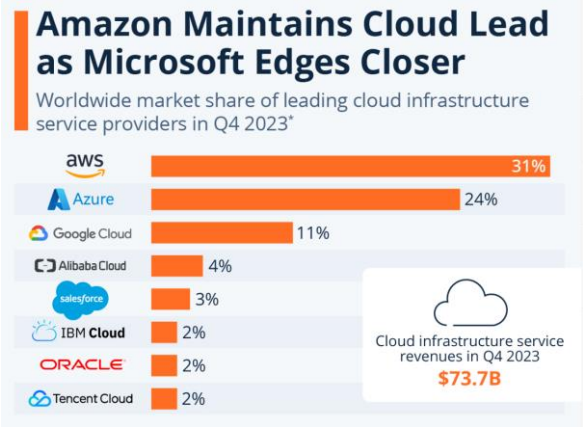
Hybridní – kombinace veřejných a privátních cloudových služeb pro větší flexibilitu a optimalizaci uživatelovy IT infrastruktury a bezpečnosti.

Komunitní – sdílí data pouze mezi vybranými organizacemi, typicky s podobnými zájmy (např. vládní instituce).

Pro firmy představují cloudové služby výhodnou příležitost, jak eliminovat velká úložiště a další nákladný software i hardware, čímž mohou šetřit firemní kapacity i finance. Firmy tak pouze platí za pronájem cloudových služeb, zatímco externí poskytovatel se stará o funkčnost systému a bezpečnost dat. Bezpečnost služeb a s ní spojená dobrá pověst je navíc v zájmu poskytovatele. **Ten proto zpravidla vkládá poměrně velké úsilí do zabezpečení cloudu, které je často na vyšší úrovni, než kdyby se o bezpečnost staral samotný uživatel. Data v cloudových úložištích jsou šifrována a zálohována standardně v několika na sobě nezávislých datacentrech, takže i kdyby došlo k selhání jednoho úložiště, uživatel data neztratí.**[2]

V současnosti lze pozorovat, že trend přechodu na cloudovou infrastrukturu mírně přibrždďuje, zvláště ve srovnání s obdobím pandemie covid-19.[3] Přesto však cloudové služby představují většinu veškeré datové infrastruktury, kdy se odhaduje, že 60 % veškerých korporátních dat je uloženo v cloudu. [4] Význam cloudové infrastruktury pro kyberbezpečnost je tedy markantní a velmi pravděpodobně (75-85 %) bude dál narůstat.

Obrázek 2: Podíl poskytovatelů na celosvětovém trhu s cloudovými službami ve 4. čtvrtletí roku 2023



Zdroj: statista.com

PŘI VÝBĚRU POSKYTOVATELE ROZHODUJE DŮVĚRYHODNOST A CITLIVOST SVĚŘOVANÝCH DAT

Cloudové služby se stávají nezbytnou součástí obchodních modelů firem a moderních společností obecně, kdy v roce 2023 využívalo cloudových služeb 45 % společností v EU a v ČR dokonce 47 %.[5] **Je téměř jisté (90–100 %), že podíl cloudových služeb bude dále narůstat a bezpečnostní hrozby s nimi spjaté je třeba reflektovat**. Největší riziko pro uživatele cloudových služeb představuje zaprvé předávání velké části kontroly nad daty spravovanými poskytovateli a dále zpracovávání dat na území jiného státu s odlišným právním řádem a přístupem k důvěrnosti dat.

Využíváním cloudových služeb se uživatel automaticky vzdává části kontroly nad svými daty. Přesto, že se poskytovatel může smluvně zavázat k převzetí zodpovědnosti za některé aspekty, část zodpovědnosti vždy zůstane na zákaznících. **Např. GDPR vnímá jako správce dat zpravidla zákazníka cloudové služby.**

Riziko zneužití dat lze snížit výběrem důvěryhodného poskytovatele, který nejlépe splňuje požadavky uživatele na bezpečnost a poskytuje služby v souladu s platnou legislativou. Před uzavřením smlouvy je nutné poskytovatele prověřit a zjistit si o něm maximum informací, včetně případných kauz, úniků dat z minulosti a způsobů jejich řešení.

Při využívání cloudových služeb je zásadní udržovat si přehled o fyzickém místě uložení dat (a jejich případném pohybu) kvůli odlišným právním řádům v jednotlivých státech, a tím pádem i rozdílné úrovni ochrany dat a soukromí uživatele. Poskytovatelé cloudových služeb disponují úložnými systémy (datovými centry) v mnoha státech, tudíž data mohou být uložena kdekoli po světě a v případě jejich zálohování i na několika místech zároveň. **Data navíc spravují zpravidla zahraniční společnosti, což ještě více komplikuje otázku, kdo všechno a podle jaké právní úpravy může s daty nakládat.** V zásadě lze říct, že z pohledu rizik vyplývajících z místa uložení a zpracování dat je nejbezpečnější zvolit takového poskytovatele cloud computingu, který ukládá a zpracovává data na území České republiky. Následují území členských států EU, respektive Evropského hospodářského prostoru (EHP). Nízkou míru netechnických rizik vyplývajících z místa uložení a zpracování dat je možné očekávat od států, kterým bylo ze strany EU uděleno tzv. adequacy decision (dle čl. 45 GDPR). Přestože adequacy decision obecně označuje státy s podobnou mírou ochrany osobních údajů a služby cloud computingu zpracovávají i jiné typy dat, lze předpokládat, že poskytuje-li právní řád dané země adekvátní ochranu osobním údajům, budou obdobným způsobem chráněna všechna data.

Naopak je třeba věnovat zvýšenou opatrnost při ukládání a zpracování dat na území států:

- **bez demokratické formy vlády;**
- **bez nezávislé soudní moci;**
- **nedbajících ochrany duševního vlastnictví;**
- **dlouhodobě či systematicky porušujících mezinárodní právo;**
- **pod mezinárodními sankcemi;**
- **považujících Českou republiku za nepřátelskou zemi, přičemž proti ní mohou vést cílené operace (např. v oblasti kybernetické bezpečnosti).**

UŽIVATEL JE NEJSLABŠÍM ČLÁNKEM, BEZPEČNOST CLOUDU NEMŮŽE ZÁVISET JEN NA POSKYTOVATELI

Neustále vzrůstající sofistikovanost kyberútoků se na poli cloudových služeb odráží v trendu sdílení zodpovědnosti nad zabezpečením cloudu mezi poskytovatelem a uživatelem. Případy narušení bezpečnosti cloudu jsou často způsobeny lidským omylem na straně uživatele, přičemž nejčastější příčinou je chybná konfigurace zabezpečení.[6] Hrozba nezodpovědného přístupu uživatele se naplno ukázala s kauzou americké banky Capital One z roku 2019, kdy podcenění bezpečnosti po přesunu podstatné části agendy na cloud nepřímo umožnilo únik citlivých dat 106 milionů klientů.[7]

Pokud uživatelé chtějí zajistit vysokou úroveň bezpečnosti svých dat, musí se na jejich ochraně sami významnou měrou spolupodílet a nespoléhat se jen na kapacity poskytovatele. Příklady modelů sdílené zodpovědnosti nabízí například Cloud Security Alliance, která poskytovatele zavazuje k zajištění bezpečnosti cloudové infrastruktury, zatímco uživatelé zodpovídají za vše „uvnitř" cloudu, včetně zabezpečení dat.[8]

Takovýto přístup od uživatelů vyžaduje investice nad rámec klasických cloudových služeb (zejména v podobě investic do erudovaného personálu), ale zato s reálnou vidinou, že vynaložený čas a finance se jim vrátí v podobě vyšší úrovně zabezpečení, a tím pádem nižší zranitelnosti vůči kyberútokům.

REGULACE CLOUDU V ČESKÉ STÁTNÍ SPRÁVĚ

V současné době jsou již služby cloud computingu v ČR hojně využívány, a to jak soukromými subjekty, tak orgány veřejné správy. Česká republika se rozhodla na tento trend reagovat vytvořením odpovídající regulace. Vše začalo v roce 2016, kdy se problematikou využívání cloudových služeb orgány veřejné správy začala zabývat pracovní skupina při Radě vlády pro informační společnost (RVIS). V listopadu 2018 tato pracovní skupina předložila vládě ke schválení Souhrnnou analytickou zprávu, která rámcově představila pravidla pro využívání služeb cloud computingu orgány veřejné správy.[9] Současně s tím se také Česká republika přihlásila k aplikaci principu „cloud first", kdy by orgány veřejné správy měly vždy zvážit, zda mají budovat vlastní digitální infrastrukturu nebo využít služeb cloud computingu.

Na základě Souhrnné analytické zprávy započaly přípravy regulace využívání cloud computingových služeb. Byla předložena novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ZoISVS), která zavedla zejména povinnost orgánů veřejné správy využívat pouze ty služby cloud computingu, které jsou zapsané v tzv. katalogu cloud computingu. Přes přechodné období, kdy bezpečnostní požadavky pro zápis služeb do katalogu stanovila metodika z dílny Ministerstva vnitra, se regulace vydáním tzv. cloudových vyhlášek posunula do stavu předpokládaného v ZoISVS. Konkrétně jde o vyhlášku č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (vyhláška o bezpečnostních úrovních), vyhlášku č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (vyhláška o vstupních kritériích) a vyhlášku č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu (vyhláška o bezpečnostních pravidlech). Ty spolu tvoří navzájem propojený a ucelený systém.

Všechny poskytovatele, jejichž služby mohou orgány veřejné správy využívat, a taktéž konkrétní nabídky služeb lze najít v katalogu cloud computingu (www.dia.gov.cz/oha/katalog-cloud-computingu/) spravovaném Digitální a informační agenturou (DIA).

BOX 2: Přehled klíčové legislativy pro využívání cloud computingových služeb orgány veřejné správy ČR

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS), a zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB).

Společně k nim byly vydány tři vyhlášky:

- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (tzv. vstupní kritéria) – účinná od 1. září 2021.
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (tzv. vyhláška o bezpečnostních úrovních) – účinná od 1. září 2021.
- Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu – účinná od 1. července 2023.

DOPORUČENÍ (STRATEGICKÁ)

Je nutné si uvědomit, že i přes veškerá možná bezpečnostní opatření je využívání služeb cloud computingu spojené s bezpečnostními riziky a mohou existovat data, u kterých není možné tato rizika z mnoha důvodů akceptovat.

- **Proto lze doporučit, aby byla před započetím využívání služby cloud computingu analyzována data z pohledu požadavků na jejich bezpečnost, a to jak z pohledu důvěrnosti, tak z pohledu integrity a dostupnosti. Zejména u těch nejkritičtějších je poté nutné zvážit, zda je vhodné a účelné zpracovávat taková data za využití cloud computingových služeb.**

Před započetím využívání služeb cloud computingu je nutné vznést otázky, jaká právní rizika z jejich využívání mohou plynout.

- **V jakých jurisdikcích budou data uložena (ať už dlouhodobě nebo krátkodobě)? Je nutné zhodnotit, jestli právní režim státu, ve kterém budou data uložena, nepředstavuje riziko pro bezpečnost informací. Uplatní se na data regulace ochrany osobních údajů?**

Organizace by měly zvážit (zvlášť s přihlédnutím na výše popsaná rizika), zda využívat cloud. Na první pohled se jeví využívání služeb cloud computingu jako velice výhodné – není nutné pořizovat vlastní infrastrukturu, o provoz i zabezpečení se starají vyškolení pracovníci poskytovatele služby, služba je pravidelně aktualizována a zákazníkovi tak odpadají náklady s tímto spojené. Je však nutné si uvědomit, že všechny tyto položky si poskytovatel služby rozpočítává do nákladů, které následně účtuje zákazníkovi, jenž platí zpravidla kontinuálně dle rozsahu využívání služby a v konečném důsledku tak může cena za využívání služeb cloud computingu přesáhnout cenu, kterou by bylo nutné zaplatit za jiné řešení.

- **Roli pro organizaci může hrát například to, jak dlouho plánuje službu provozovat, nakolik je provoz služby technicky náročný, k čemu chce službu cloud computingu využít či zda bude využívat službu ve stejné intenzitě neustále nebo očekává v jejím využívání výkyvy ve vytíženosti atd. Doporučujeme proto provést analýzu, kde budou zhodnoceny náklady spojené s provozem služby jak pomocí cloudového řešení, tak vlastními silami (tzv. on premise řešení).**

DOPORUČENÍ (MANAŽER KB)

Při využívání služby cloud computingu předáváte svá data do moci poskytovatele. Je tedy třeba mít k poskytovateli a službě cloud computingu důvěru. Proto je nutné vybrat takového poskytovatele služeb cloud computingu, který je maximálně transparentní v ohledu nabízených služeb a vlastnické struktury a umožní ověření svého řešení bezpečnosti informací (např. odkazem na příslušné certifikáty a mezinárodně uznávané standardy).

- **Zvýšenou pozornost je pak vždy nutné věnovat tomu, jak poskytovatel řeší kontinuitu poskytování služby, obnovu po havárii (BC/DR) a převoditelnost dat k jinému poskytovateli v případě nutnosti přenést data vložená do služby cloud computingu.**

Ověřte a řiďte, kdo bude mít přístup k datům. Stejně jako je nutné provést úvahu nad tím, kde se budou data nacházet, je nutné se také zamyslet nad tím, kdo k nim bude přistupovat, a to jak na straně poskytovatele služby cloud computingu, tak na straně jejího zákazníka.

- **Na straně poskytovatele je nutné zabezpečit zejména to, kdo přistupuje k datům (obzvlášť nezašifrovaným), na jak dlouho a z jakého důvodu. O všech těchto přístupech by měl být veden auditovatelný záznam, který by měl zákazník mít možnost periodicky kontrolovat.**
- **Na straně zákazníka je pak nutné nastavit přístupy tak, aby vždy odpovídaly jeho reálným potřebám a současně nebyly jednotlivým uživatelům zpřístupněny funkcionality způsobilé narušit využívání služby.**

Pečlivě nastavte jednotlivé parametry služby cloud computingu. Chybná konfigurace je častou příčinou kybernetických incidentů.

- **Postupujte při nastavování služby dle vašich požadavků na zajištění bezpečnosti informací a v souladu s doporučeními poskytovatele cloud computingu.**

DOPORUČENÍ (KONCOVÝ UŽIVATEL)

Koncový uživatel by měl přemýšlet nad tím, co dává do cloudu a využívat službu cloud computingu jen k určenému účelu. Do cloudu by se měla vkládat jen dovolená data.

- **Nehledě na to, jak je služba cloud computingu bezpečná, je vždy nutné ji využívat jen k určeným účelům a v rámci pravidel nastavených vaší organizací.**

Stejně jako u mnoha dalších aspektů kybernetické bezpečnosti je i u využívání cloudových služeb klíčová bezpečnost přihlašování a ověřování uživatele.

- **Při zacházení s přístupovými údaji ke službě cloud computingu je nutné být stejně opatrný jako při zacházení s jakýmikoli jinými přístupovými údaji. Je tedy nutné např. volit bezpečná hesla, pro přihlašování využívat bezpečných sítí, využívat vícefaktorovou autentizaci a s nikým své přihlašovací údaje nesdílet. Výrazně se tak omezí možnost, že bude ke službě cloud computingu přistoupeno neoprávněně.**

Vzhledem k omezené kontrole a informovanosti nad cloudovou službou je o to víc důležité mít se na pozoru před projevy různých podezřelých aktivit a neobvyklého chování služby.

- **Pokud narazíme při využívání služby cloud computingu na cokoliv podezřelého, je lepší to vždy nahlásit osobě, které je dohled nad využíváním služby cloud computingu svěřen.**
- **V případě služeb cloud computingu je vždy s ohledem na omezenou kontrolu dat svěřených jejich poskytovateli nutné postupovat při řešení bezpečnostních incidentů bez zbytečných odkladů. Včasné upozornění na podezřelé chování služby cloud computingu ze strany uživatelů může být klíčové.**

PŘÍLOHA 1: TYPY CLOUDOVÝCH SLUŽEB

Software jako služba (Software as a Service – SaaS)

- Poskytování/pronájem licencí k softwarovým aplikacím – uživatel si kupuje přístup k aplikaci, ne aplikaci samotnou.

Infrastruktura jako služba (Infrastructure as a Service – IaaS)

- Poskytování/pronájem virtuálních hardwarových zdrojů (tj. infrastruktury) – vhodné pro uživatele, kteří vlastní software (nebo licence k němu), ale nechtějí provozovat a spravovat hardware.

Backend jako služba (Backend as a Service – BaaS)

- Alternativa k mobilnímu middlewaru a tradičnímu backendu – slouží k jednoduchému propojení mobilních aplikací s cloudovým backendovým úložištěm nebo s API backendových aplikací za účelem ukládání, správy a přístupu k datům přes cloud.

Databáze jako služba (Database as a Service – DbaaS):

- Zaměřena na ukládání a správu strukturovaných dat v cloudu s cílem poskytovat tradiční funkce relačních databázových systémů, ale v kombinaci s výhodami cloudu.

Funkce jako služba (Function as a Service – FaaS)

- Umožňuje vyvíjet, spouštět a spravovat funkce aplikace bez nutnosti vytvářet a udržovat komplexní infrastrukturu, která je jinak pro vývoj aplikací nutná.

Umělá inteligence jako služba (AI as a Service – AiaaS)

- Umožňuje experimentovat s umělou inteligencí bez nutnosti vysokých počátečních investic a expertizy uživatele.

Platforma jako služba (Platform as a Service – PaaS)

- Poskytování/pronájem kompletní IT infrastruktury spolu se standardními softwarovými platformami (např. Salesforce.com, Google App Engine atd.).

PŘÍLOHA 2: SHRNUTÍ OBSAHU CLOUDOVÝCH VYHLÁŠEK

CO JSOU TO CLOUDOVÉ VYHLÁŠKY?

Jako cloudové vyhlášky jsou označovány vyhlášky, které mají stanovit konkrétní pravidla pro nový systém cloud computingu pro veřejnou správu, podle zákona o kybernetické bezpečnosti a zákona o informačních systémech veřejné správy. Jedná se o vyhlášku č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu, vyhlášku č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, vyhlášku č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu a vyhlášku č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.

CO STANOVÍ VYHLÁŠKA O POŽADAVCÍCH PRO ZÁPIS DO KATALOGU CLOUD COMPUTINGU?

Vyhláška o vstupních kritériích (vyhláška č. 316/2021 Sb.) stanoví požadavky, které musí poskytovatel cloudových služeb splnit, aby mohl vstoupit do katalogu cloud computingu a nabídnout tak své služby orgánům veřejné správy. Tato kritéria se liší podle příslušné bezpečnostní úrovně služby (vysvětlení viz níže). Pokud poskytovatel služeb stanovené požadavky splní a doloží potřebné dokumenty, bude mu umožněno nabízet orgánům veřejné správy cloudové služby. Splnění těchto podmínek ověřuje DIA ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Tento proces je tzv. ex ante kontrola.

CO STANOVÍ VYHLÁŠKA O BEZPEČNOSTNÍCH PRAVIDLECH?

Vyhláška o bezpečnostních pravidlech (vyhláška č. 190/2023 Sb.) stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné správy, které využívají cloudové služby. Jde tedy o seznam bezpečnostních požadavků, jejichž splnění musí orgány veřejné správy zajistit, pokud využívají cloudových služeb. Tato bezpečnostní pravidla budou často součástí výběrového řízení na poskytnutí cloudových služeb. Splnění těchto podmínek bude kontrolováno ze strany NÚKIB. Kontrola bude probíhat až v době, kdy bude služba poskytována. Každá z bezpečnostních úrovní má stanovena bezpečnostní opatření, přiměřeně přísná podle příslušné bezpečnostní úrovně.

CO STANOVÍ VYHLÁŠKA O BEZPEČNOSTNÍCH ÚROVNÍCH?

Vyhláška o bezpečnostních úrovních (vyhláška č. 315/2021 Sb.) stanovuje pravidla, podle jakých se informační systémy orgánů veřejné správy, které by měly být provozovány v cloudu, rozřazují do příslušných bezpečnostních úrovní. Podle dopadů narušení bezpečnosti informací budou informační systémy rozřazeny do čtyř bezpečnostních úrovní (1 – nízká, 2 – střední, 3 – vysoká, 4 – kritická). Příslušně zařazený systém bude moci využít pouze ty nabídky služeb cloud computingu, které jsou zařazeny do stejné nebo vyšší bezpečností úrovně.

POUŽITÉ ZDROJE

[1] Aggarwai, Gaurav. 2021. How The Pandemic Has Accelerated Cloud Adoption. Forbes. How The Pandemic Has Accelerated Cloud Adoption (forbes.com)

[2] Montgomery, Tommy. 2021. Why your data is safer in the cloud than on premises. TechBeacon. Why your data is safer in the cloud than on premises | TechBeacon

[3] Vailshery, Lionel Sujay. 2023. Current enterprise public cloud adoption worldwide from 2017 to 2023, by service. Statista. Enterprise public cloud service usage worldwide 2023 | Statista

[4] Flynn, Jack. 2023. 25 amazing cloud adoption statistics [2023]: cloud migration, computing, and more. Zippia. 25 Amazing Cloud Adoption Statistics [2023]: Cloud Migration, Computing, And More - Zippia

[5] Eurostat. 2023. 45% EU enterprises bought cloud services in 2023. 45% EU enterprises bought cloud services in 2023 - Eurostat (europa.eu)

[6] GRC World Forums. 2023. Cloud data breaches caused mostly by human error. Cloud data breaches caused mostly by human error | News | GRC World Forums

[7] Schroeder, Pete. 2020. Capital One to pay $80 million fine after data breach. Reuters. Capital One to pay $80 million fine after data breach | Reuters

[8] The Importance of the Shared Responsibility Model for Your Data Security Strategy. 2023. Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2023/10/17/the-importance-of-the-shared-responsibility-model-for-your-data-security-strategy

[9] Rada vlády pro informační společnost. 2024. Rada vlády pro informační společnost - Ministerstvo vnitra České republiky (mvcr.cz)