Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j.: 7226/2022-NÚKIB-E/310• BRNO • 03. LISTOPAD 2022

STRATEGICKÁ ANALÝZA

CLOUDY UMOŽNUJÍ SNÍŽENÍ NÁKLADŮ A SNADNÝ VZDÁLENÝ PŘÍSTUP, ZA CENU ZTRÁTY PLNÉ KONTROLY NAD DATY

SHRNUTÍ

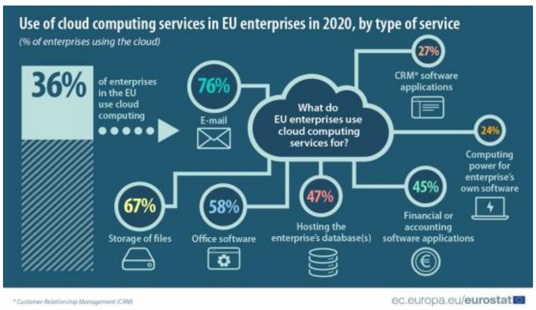
- **Cloudovými službami se rozumí služby umožňující vzdálený samoobslužný přístup k výpočetním zdrojům, které jsou zpravidla schopné se přizpůsobit potřebám zákazníků. Velké množství firem i státních institucí po celém světě využívá cloudových služeb. Pandemie viru covid-19 tento trend výrazně urychlila.**
- **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, a je tak 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 třeba brát v potaz i to, v jaké zemi jeho společnost sídlí a v jaké zemi 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. S ohledem na nedostatečnou regulaci však není jejich pořizování a využívání podrobeno adekvátním kontrolním procesům, které jsou s ohledem na rizika spojená s využíváním služeb cloud computingu potřebné.**
- **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, jak citlivá data ukládat na cloud.**

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 tak nejsou uložena na fyzickém „domácím" úložišti (typicky pevném disku), ale uživatel je svěřuje do správy externího poskytovatele cloudové služby, který data shromažďuje ve vzdálených serverech po celém světě.

Obrázek 1: Využívání cloudových služeb v EU v roce 2020



Zdroj: Eurostat

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

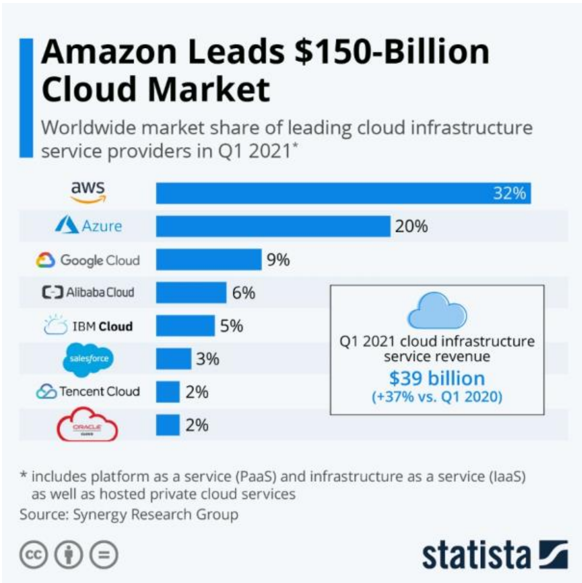
Hybridní – kombinace veřejných a privátních cloudových služeb pro větší flexibilitu a optimalizaci uživatelovy IT infrastruktury a bezpečnosti

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 tak často na vyšší úrovni, než kdyby se o bezpečnost staral samotný uživatel. Data v cloudových úložištích jsou šifrována a zálohována standartně v několika na sobě nezávislých datacentrech, takže i kdyby došlo k selhání jednoho úložiště, uživatel data neztratí.**[2]

Využívání cloudových služeb (cloud computing) od roku 2010 neustále roste [3] a je téměř jisté (90–100 %), že tento trend bude pokračovat i nadále, čemuž zásadně napomáhá i proměna přístupu k práci v důsledku pandemie covid-19.

Obrázek 2: Podíl poskytovatelů na celosvětovém trhu s cloudovými službami v 1. čtvrtletí 2021



Zdroj: Statista

VÝBĚR POSKYTOVATELE: ROZHODUJE DŮVĚRYHODNOST A CITLIVOST SVĚŘOVANÝCH DAT

Cloudové služby se stávají nezbytnou součástí obchodních modelů firem a moderních společností obecně – v roce 2021 využívalo cloudových služeb 41 % společností v EU, v ČR dokonce 44 %.[4] Celkový podíl cloudových služeb na celosvětovém IT trhu pak v témže roce činil 9,1 % a do roku 2024 je predikován nárůst na 14,2 %.[5] **Je proto 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 za prvé předávání velké části kontroly nad daty poskytovateli a za druhé zpracovávání dat na území jiného státu s odlišným přístupem k bezpečnosti 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 zákazníkovi. **Například GDPR vnímá jako správce dat z pravidla 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 co nejvíc 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 (viz Box 2). Poskytovatelé cloudových služeb disponují úložnými systémy (datovými centry) v mnoha státech, a data tak mohou být uložena kdekoli po světě, v případě jejich zálohování i na několika místech zároveň. **Data navíc spravují zpravidla zahraniční společnosti (především z USA), což ještě více komplikuje otázku, kdo všechno a podle jaké právní úpravy může s daty nakládat.**

Až do roku 2013 panovalo obecné přesvědčení, že data uložená v cloudových data centrech patří výhradně samotným uživatelům a jedině oni sami s nimi mohou libovolně zacházet. **Soudní spor společnosti Microsoft s americkou vládou z let 2013–2018 (viz Box 2) ovšem tento předpoklad výrazně narušil a otevřel diskusi o šedé zóně protiřečících si právních výkladů, kterou se doposud nepodařilo vyjasnit ani prostřednictvím úpravy zákonů o cloudových službách v EU i USA.**

PROBLEMATICKÉ PRÁVNÍ RÁMCE EU A USA VE VZTAHU K OSOBNÍM DATŮM

Spojené státy představují klíčovou zemi pro evropský cloud computing. Jednak jsou sídlem tří největších poskytovatelů (Microsoft, Amazon, Google), [6] a zároveň, ve srovnání s Čínou, (která nabízí druhou největší nabídku poskytovatelů), disponuje demokratickým státním zřízením a právním státem. **Přesto mají Evropská Unie a Spojené státy americké dlouhodobý problém sjednotit své cloudové legislativy týkající se ochrany osobních údajů.** Zatímco v rámci EU o nastavení soukromí rozhoduje fyzické místo uložení dat podle jurisdikce jednotlivých členských států a od roku 2018 pozici uživatele posiluje Obecné nařízení o ochraně osobních údajů (GDPR),[7] v USA od stejného roku platí tzv. CLOUD Act, na jehož základě musí američtí poskytovatelé v odůvodněných případech data vydat americké vládě, a to bez ohledu na to, zda se data fyzicky nachází na území USA.[8] CLOUD Act tedy nadřazuje americké zájmy nad právní úpravu v EU a dostává se tím do přímého střetu s GDPR. Uživatelé amerických cloudových služeb si tudíž nemohou být jisti, zda jejich data nebudou vydána americkým úřadům.[9]

BOX 2: Soudní spor společnosti Microsoft s americkou vládou 2013–2018

V souvislosti s vyšetřováním případu obchodování s drogami vydal americký soud v prosinci 2013 příkaz společnosti Microsoft zpřístupnit orgánům činným v trestním řízení data z e-mailového účtu, která byla uložena v datovém centru v irském Dublinu. Microsoft se proti rozhodnutí bránil soudní cestou s argumentací, že ochrana dat podléhá právnímu řádu dotyčného státu, kde jsou data fyzicky uložena, tedy Irska. Americká vláda se zaštiťovala svým právem získat od Microsoftu jakákoliv data odkudkoliv na světě, jelikož se jedná o americkou společnost se sídlem na území USA, která je primárně podřízena domácí jurisdikci.

Vleklý soudní spor vyřešilo až přijetí nového zákona CLOUD Act (Clarifying Lawful Overseas Use of Data Act), podle něhož jsou od března 2018 americké technologické společnosti povinny poskytnout americkým úřadům požadovaná data bez ohledu na to, zda jsou fyzicky uložena na území USA, nebo v zahraničí.

Američtí poskytovatelé cloudových služeb se kvůli přijetí CLOUD Act a GDPR ocitli v komplikované situaci, kdy se při působení v EU musí řídit oběma právními úpravami, přestože se vzájemně vylučují. Ačkoliv nesoulad právních úprav lze do jisté míry a za určitých podmínek ošetřit standardními smluvními doložkami,[10] neexistuje žádné kompromisní řešení s oporou v zákonech (dosavadní dohody Privacy Shield a Safe Harbor byly zrušeny Evropským soudním dvorem v důsledku soudního přezkumu – viz Příloha 3). Vzhledem ke skutečnosti, že vymáhání dodržování GDPR u zahraničních subjektů může být obtížné, nelze vyloučit (25–50 %) tendenci poskytovatelů řídit se domácí právní úpravou (v případě amerických dodavatelů tedy CLOUD Act). [11] **Mezi evropskou a americkou stranou existuje vůle a snaha situaci řešit a v současnosti se připravuje nová dohoda.**[12] **Lze však očekávat, že práce na nové dohodě se protáhnou minimálně do konce roku, pravděpodobně (55–75 %) budou trvat i déle. Pokud se uživatel v současnosti rozhodne využít cloudové služby prostřednictvím amerického poskytovatele, nemá tak zatím právní jistotu, že jeho soukromí a ochrana dat nebudou narušeny americkými úřady.** Alternativou je volba poskytovatele se sídlem i datovými centry v EU, který je vázán pouze dodržováním GDPR, a to především v případě nutnosti ochrany mimořádně citlivých dat (např. bankovní sektor, zdravotnictví, osobní data občanů).

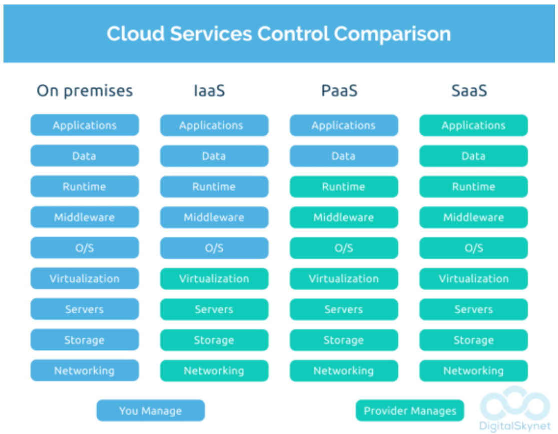
UŽIVATEL JE NEJSLABŠÍM ČLÁNKEM, BEZPEČNOST CLOUDU NEMŮŽE ZÁVISET JEN NA POSKYTOVATELI

Neustále vzrůstající sofistikovanost kyberútoků se na poli cloudových služeb odráží v trendu sdílení zodpovědnosti nad zabezpečením cloudu mezi poskytovatelem a uživatelem. Dle odhadů společnosti Gartner je drtivá většina (až 95 %)[13] případů narušení bezpečnosti cloudu způsobena lidským omylem na straně uživatele, přičemž nejčastější příčinou je chybná konfigurace zabezpečení.[14] 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.[15]

Pokud uživatelé chtějí zajistit co možná nejvyšší úroveň bezpečnosti svých dat, musí se na jejich ochraně sami významnou měrou spolupodílet a nespoléhat se jen na kapacity poskytovatele. Příklad modelu 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.[16]

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.

Obrázek 3: Model sdílené zodpovědnosti (Shared Responsibility Model) – [větší rozlišení]



Zdroj: dev.to

IMPLIKACE PRO ČR: REGULACE CLOUDU VE STÁTNÍ SPRÁVĚ SE V SOUČASNOSTI VYTVÁŘÍ

V současné době jsou již služby cloud computingu v ČR hojně využívány, a to jak soukromými subjekty, tak orgány veřejné moci. **S ohledem na chybějící regulaci však není jejich pořizování a využívání podrobeno adekvátním kontrolním procesům, které jsou s ohledem na rizika spojená s využíváním služeb cloud computingu potřebné.** Zejména riziko ztráty přístupu k datům či jejich zpracovávání mimo území EU je natolik významné, že by nemělo být opomíjeno. Obzvláště za situace, kdy velcí poskytovatelé cloud computingových služeb při prodeji svých služeb neumožňují jednotlivým zákazníkům vyjednat si více vyhovující podmínky poskytování cloud computingové služby. **Situaci komplikuje fakt, že největší poskytovatelé služeb cloud computingu zpravidla neprodávají své služby sami, ale činí tak přes síť přeprodejců.** Zákazník tedy neuzavírá smlouvu přímo s poskytovatelem služby, což činí některé následné kroky (zákaznický audit, změny smluvních ujednání, kontrola zacházení se zákaznickými daty apod.) složitějšími. Nutno podotknout, že se jedná o zcela běžnou strategii, která sama o sobě nemusí znamenat problematický provoz služby cloud computingu, nicméně v případě komplikací může pro zákazníka představovat významné překážky.

BOX 3: Přehled klíčové legislativy pro využívání cloud computingových služeb orgány veřejné správy ČR

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

Společně k nim byly vydány dvě vyhlášky a třetí se v současnosti připravuje:

- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (tzv. vstupní kritéria) - ÚČINNÁ OD 1. 9. 2021
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (tzv. vyhláška o bezpečnostních úrovních) - ÚČINNÁ OD 1. 9. 2021
- Vyhláška o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci (pracovní název) – předpokládaná účinnost v prvním čtvrtletí roku 2023

V rámci ČR je o regulaci využívání služeb cloud computingu orgány veřejné správy jednáno již od roku 2016, kdy se touto problematikou začala zabývat pracovní skupina při Radě vlády pro informační společnost (RVIS). V listopadu 2018 pracovní skupina předložila vládě ke schválení Souhrnnou analytickou zprávu, která rámcově představila pravidla pro využívání služeb cloud computingu orgány veřejné správy. Současně s tím se také Česká republika přihlásila k aplikaci principu „cloud first" – orgány veřejné správy by měly vždy zvážit, zdali mají budovat vlastní digitální infrastrukturu, nebo využít služeb cloud computingu.

Na základě Souhrnné analytické zprávy započaly přípravy regulace využívání cloud computingových služeb. Mezi hlavní subjekty zapojené do legislativních prací patří Ministerstvo vnitra a NÚKIB, na jejich tvorbě se však podílela a podílí celá řada dalších subjektů, ať už ze soukromého či veřejného sektoru (viz Box 3).

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, zdali je vhodné a účelné zpracovávat taková data za využití cloud computingových služeb.**

Před započetím využívání služeb cloud computingu je nutné vzít v potaz, 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, a zákazník 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 zdali 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 KYBERNETICKÉ BEZPEČNOSTI)

Při využívání služby cloud computingu předáváte svá data do moci poskytovatele. Je tedy třeba mít k poskytovateli a službě cloud computingu důvěru. Proto je třeba 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 potřeby 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 nastavovaní 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 jakýmikoliv 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 (= 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 expertízy uživatele

Platforma jako služba (Platform as a Service – PaaS)

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

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. Kromě již účinné vyhlášky č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu, se má jednat ještě o trojici dalších vyhlášek, které stanoví pravidla pro zápis do katalogu cloud computingu, bezpečnostní pravidla pro využívání služeb cloud computingu a bezpečnostní úrovně informačních systémů podle závažnosti dopadů narušení bezpečnosti informací.

CO STANOVÍ VYHLÁŠKA O VSTUPNÍCH KRITÉRIÍCH?

Vyhláška o vstupních kritériích (č. 316/2021 Sb.) stanoví požadavky, které musí poskytovatel cloudových služeb splnit, aby mohl vstoupit do katalogu eGovernment cloudu a nabídnout tak své služby orgánům veřejné moci. Tato kritéria budou rozdílná podle příslušné bezpečnostní úrovně služby (vysvětlení viz níže). Pokud poskytovatel služeb stanovené požadavky splní a doloží potřebné dokumenty, bude mu umožněno nabízet orgánům veřejné moci cloudové služby. Splnění těchto podmínek bude ověřovat Ministerstvo vnitra ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost (dále Úřad). Tento proces je tzv. ex ante kontrola.

CO STANOVÍ VYHLÁŠKA O BEZPEČNOSTNÍCH PRAVIDLECH?

Vyhláška o bezpečnostních pravidlech stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci, které budou chtít cloudové služby využívat. Jde tedy o seznam bezpečnostních požadavků, jejichž splnění budou muset orgány veřejné moci zajistit, pokud budou chtít využít cloudových služeb. Tato bezpečnostní pravidla budou často součástí výběrového řízení na poskytnutí cloudových služeb. Splnění těchto podmínek bude kontrolováno ze strany Ministerstva vnitra a Úřadu. Kontrola bude probíhat až v době, kdy bude služba poskytována. Každá z bezpečnostních úrovní bude mít stanovena bezpečnostní opatření, přiměřeně přísná podle příslušné bezpečnostní úrovně.

CO STANOVÍ VYHLÁŠKA O BEZPEČNOSTNÍCH ÚROVNÍCH?

Vyhláška o bezpečnostních úrovních (č. 315/2021 Sb.) stanovuje pravidla, podle jakých se informační systémy orgánů veřejné moci, které by měly být provozovány v cloudu, budou rozřazovat 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.

PŘÍLOHA 3: ANALÝZA ÚOOÚ KAUZ SCHREMS I A SCHREMS II

Neplatnost rozhodnutí Komise o tzv. Safe Harbor (Schrems I)[17]

Soudní dvůr Evropské unie v rozsudku ve věci C-362/14 Maximillian Schrems v. Data Protection Commissioner ze dne 6. října 2015 prohlásil za neplatné rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států amerických, na základě kterého bylo dosud možné předávat osobní údaje do Spojených států americkým společnostem, které se zavázaly dodržovat zásady „bezpečného přístavu“ (Safe Harbor).

Spojené státy americké se řadí k tzv. třetím zemím s nedostatečnou úrovní ochrany osobních údajů. Jako zvláštní nástroj k zajištění odpovídající úrovně ochrany osobních údajů i po jejich předání příjemci do Spojených států amerických vytvořila Evropská komise společně s vládními orgány Spojených států amerických v roce 2000 systém „bezpečného přístavu“ („Safe Harbor“), definovaného rozhodnutím Komise ze dne 26. července 2000. Na základě dnes již zrušeného rozhodnutí Komise o „bezpečném přístavu“ bylo možné volně předávat osobní údaj z EU do USA společnostem, které se přihlásily k dodržování principů bezpečného přístavu. Z pohledu EU se de facto jednalo o závazek USA, že předávaným údajům bude zajištěna ze strany této společnosti odpovídající úroveň ochrany podle stejných principů, kterými se řídí ochrana údajů v EU (omezení účelu, kvalita a přiměřenost zpracovávaných dat, bezpečnost, transparentnost, omezení dalšího předávání atd.).

Odhalení sledovacích programů Spojených států (PRISM apod.), v rámci, kterých docházelo k předávání údajů občanů Evropské unie prostřednictvím některých internetových společností americkým veřejným orgánům, mělo negativní dopad na důvěru ve způsob zpracování a ochrany osobních údajů v USA.

K tématu bezpečnosti předávaných osobních údajů do USA se v minulosti vyjádřila Evropská komise ve sdělení Evropskému parlamentu a Radě ze dne 27. listopadu 2013 („Obnovení důvěry v toky údajů mezi EU a USA“) a dále také Evropský parlament v usnesení Evropského parlamentu ze dne 21. února 2014 o programu agentury NSA (USA) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí (2013/2188(INI). Úřad od té doby upozorňoval vývozce osobních údajů do USA, že účast příjemce osobních údajů v programu Safe Harbor sama o sobě fakticky nemůže zajistit odpovídající úroveň ochrany osobních údajů ve Spojených státech amerických, a doporučoval předávání zajistit prostřednictvím jiných nástrojů.

K rozsudku ESD se ve svém prohlášení ze dne 16. října 2015 vyjádřila i Pracovní skupina podle čl. 29 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (WP 29). WP 29 především ve svém stanovisku vyzvala členské státy EU a evropské instituce k tomu, aby byly zahájeny diskuze s americkými úřady za účelem nalezení politického, právního a technického řešení, které by umožnilo pokračovat v předávání dat z EU do USA.

Do doby, než bude přijata ze strany orgánů Evropské unie alternativa k programu Safe Harbor, je nutné zajistit předání osobních údajů do Spojených států amerických, které se ukáže být nezbytně nutným k naplnění stanovených účelů, jinými nástroji, jimiž lze zajistit odpovídající úroveň ochrany osobních údajů ve třetích zemích s nedostatečnou úrovní ochrany osobních údajů, mezi kterými se jako nejvhodnější jeví standardní smluvní doložky nebo závazná podniková pravidla. V podobném smyslu se vyjádřila i WP 29 ve svém stanovisku, když konstatovala, že předávání dat je stále možné na základě standardních smluvních doložek nebo závazných podnikových pravidel.

V souvislosti s využitím standardních smluvních doložek Úřad doporučuje, aby správce/vývozce údajů jako jedna ze smluvních stran vždy důkladně zvážil rizika související s předáváním a prověřil, zda je vývozce údajů schopen dodržet zásady, k nimž se ve standardních smluvních doložkách zavázal. Je totiž především odpovědností vývozce údajů vyvinout přiměřené úsilí k tomu, aby zjistil, že je dovozce údajů schopen dostát svým závazkům vyplývajícím z doložek.

Rozsudek SDEU C-311/18 (Schrems II) a jeho důsledky[18]

Prováděcí rozhodnutí Komise ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí bylo prohlášeno za neplatné rozsudkem Soudního dvora Evropské unie ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II) ze dne 16. července 2020. Nadále tak již není možné předávat osobní údaje do USA na základě Štítu soukromí.

Rozsudek Soudního dvora konstatoval, že ve světle Listiny základních práv Evropské unie musí vhodné záruky podle čl. 46 obecného nařízení o ochraně osobních údajů zajistit předaným osobním údajům ve třetí zemi ochranu v zásadě rovnocennou ochraně poskytované obecným nařízením.

Vycházeje z tohoto konstatování dospěl Evropský soudní dvůr k závěru, že Rozhodnutí Komise 2010/87 ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES je platné. Zároveň však Evropský soudní dvůr zdůraznil, že pokud konkrétní smlouva obsahující dané standardní smluvní doložky nezajišťuje předaným osobním údajům ve třetí zemi ochranu v zásadě rovnocennou ochraně poskytované obecným nařízením, pak je na odpovědnosti vývozce a dovozce osobních údajů, aby poskytli dodatečné záruky, které požadovanou ochranu osobních údajů ve třetí zemi zajistí.

Evropský soudní dvůr zároveň vyžaduje, aby dozorové orgány jednotlivých členských zemí Evropské unie postupovaly při čl. 46 obecného nařízení koordinovaně ve spolupráci s Evropským sborem pro ochranu osobních údajů. Další informace lze nalézt v prohlášení Evropského sboru pro ochranu osobních údajů ze dne 17. července 2020 a v dokumentu Často kladené otázky k rozhodnutí Rozsudek Soudního dvora Evropské unie ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems.

Podrobně se Evropský sbor pro ochranu osobních údajů důsledkům uvedeného rozsudku věnuje v Doporučení Sboru 1/2020 k opatřením doplňujícím stávající nástroje předávání osobních údajů pro zajištění EU úrovně ochrany osobních údajů. V uvedeném doporučení Sbor popisuje v několika krocích, jak má postupovat správce (příp. zpracovatel), který hodlá předávat osobní údaje do třetí země s nedostatečnou úrovní ochrany osobních údajů, aby zajistil předaným údajům ve třetí zemi úroveň ochrany „v zásadě rovnocennou“ s unijní úrovní ochrany osobních údajů, jak ji vyžaduje ustanovení čl. 46 obecného nařízení vyložené uvedeným rozhodnutím SDEU:

1. Správce musí předně skutečně znát okolnosti svého předání a uplatnit na předání jako na samostatnou operaci zpracování všechny zásady definované čl. 5 obecného nařízení, tzn. správce musí především vědět komu a do kterých zemí hodlá data předat, musí určit účel předání osobních údajů a vymezit relevantní údaje, které je nezbytné pro naplnění stanoveného účelu předat do třetí země.

2. Správce musí zvolit jeden z nástrojů pro předání vyjmenovaných v čl. 46 obecného nařízení, přičemž, pokud správce není členem skupiny disponující schválenými závaznými podnikovými pravidly, je v současné době stále jedinou schůdnou cestou použití standardních smluvních doložek podle rozhodnutí Evropské komise.

3. Správce musí v kontextu daného předání, nejlépe ve spolupráci s potenciálním dovozcem osobních údajů, zhodnotit, zda legislativa třetí země nenaruší úroveň ochrany předaných osobních údajů takovým způsobem, že ani použití zvoleného nástroje podle čl. 46 samo o sobě nezajistí vhodné záruky ochrany předaných osobních údajů. Především se správce musí soustředit na zhodnocení otázky, zda právní řád třetí země umožňuje jejím orgánům veřejné moci přístup k předaným osobním údajům v rozsahu, který jde nad rámec toho, co je obvyklé v demokratické společnosti, v čemž mu mohou pomoci Doporučení Sboru 2/2020 k zásadním zárukám přiměřeného přístupu k osobním údajům.

4. V případě, že správce dojde k závěru, že pro dané předání do třetí země neposkytuje zvolený nástroj podle čl. 46 dostatečné záruky pro zajištění „v zásadě rovnocenné“ ochrany předaných osobních údajů, musí správce, zpravidla ve spolupráci s dovozcem, přijmout doplňková opatření, která navýší záruky na požadovanou úroveň. V přílohách uvedeného Doporučení Sboru 1/2020 jsou uvedeny příklady možných technických, smluvních a organizačních opatření. Pokud správce nepřijme nebo nenalezne taková doplňková opatření, nezbude mu nic

jiného než předání nerealizovat, resp. v případech již probíhajících předávání toto zastavit nebo oznámit danou skutečnost příslušnému dozorovému úřadu, který rozhodne o zastavení předávání.

5. Správce musí posléze ve vhodných intervalech znovu zhodnotit, zda v právním řádu dané třetí země nedošlo k nepříznivému vývoji vzhledem k úrovni ochrany předávaných údajů, a zda tedy není nutné nalézt a přijmout ještě jiná doplňková opatření.

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] Ikink, Roy. 2021. 25 cloud trends for 2021 and beyond. Accenture. Top cloud trends for 2021 and beyond | Accenture., Synergy. 2022. Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total, Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total | Synergy Research Group (srgresearch.com)

[4] Eurostat. 2022. Cloud computing - statistics on the use by enterprises. Cloud computing - statistics on the use by enterprises - Statistics Explained (europa.eu)

[5] Costello, Katie. 2020. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021. Gartner. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021

[6] Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total, Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total | Synergy Research Group (srgresearch.com)

[7] Novák, Patrik. 2018. Cloudová úložiště z pohledu GDPR. Kropáček Legal. Cloudová úložiště z pohledu GDPR | Právo pro podnikatele (pravopropodnikatele.cz)

[8] Eelectronic Privacy Information Center. 2021. The CLOUD Act. EPIC - The CLOUD Act

[9] Grande, Allison. 2020. US Courts Open To Demands For EU Data, But Risks Loom. LAW360. US Courts Open To Demands For EU Data, But Risks Loom - Law360

[10] Úřad pro ochranu osobních údajů. 2021. Standartní smluvní doložky. Standardní smluvní doložky: Úřad pro ochranu osobních údajů (uoou.cz)

[11] ibidem.

[12] Česká televize. 2022. Evropská unie a USA našly principiální shodu ohledně předávání uživatelských dat do Spojených států. Evropská unie a USA našly principiální shodu ohledně předávání uživatelských dat do Spojených států — ČT24 — Česká televize (ceskatelevize.cz)

[13] Rundle, James. 2019. Human Error Often the Culprit in Cloud Data Breaches. The Wall Street Journal. Human Error Often the Culprit in Cloud Data Breaches - WSJ

[14] NetApp. 2021. What are Cloud Security Breaches? Top Cloud Security Breaches and How to Protect Your Organization (netapp.com)

[15] 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

[16] Amazon Web Services. 2021. Shared Responsibility Model. Shared Responsibility Model - Amazon Web Services (AWS)

[17] Úřad pro ochranu osobních údajů. 2015. Neplatnost rozhodnutí Komise o tzv. Safe Harbor - doporučení Úřadu. Neplatnost rozhodnutí Komise o tzv. Safe Harbor - doporučení Úřadu: Názory a rozhodnutí Úřadu: Úřad pro ochranu osobních údajů (uoou.cz)

[18] Úřad pro ochranu osobních údajů. 2020. Rozsudek SDEU C-311/18 (Schrems II) a jeho důsledky. Rozsudek SDEU C-311/18 (Schrems II) a jeho důsledky: Úřad pro ochranu osobních údajů (uoou.cz)

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
Zelená TLP: GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP: CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*25–50 %*
Nepravděpodobně	*15–20 %*
Velmi nepravděpodobně	*0–10 %*