Bezpečnost cloudových služeb

2019
www.pwc.com

pwc

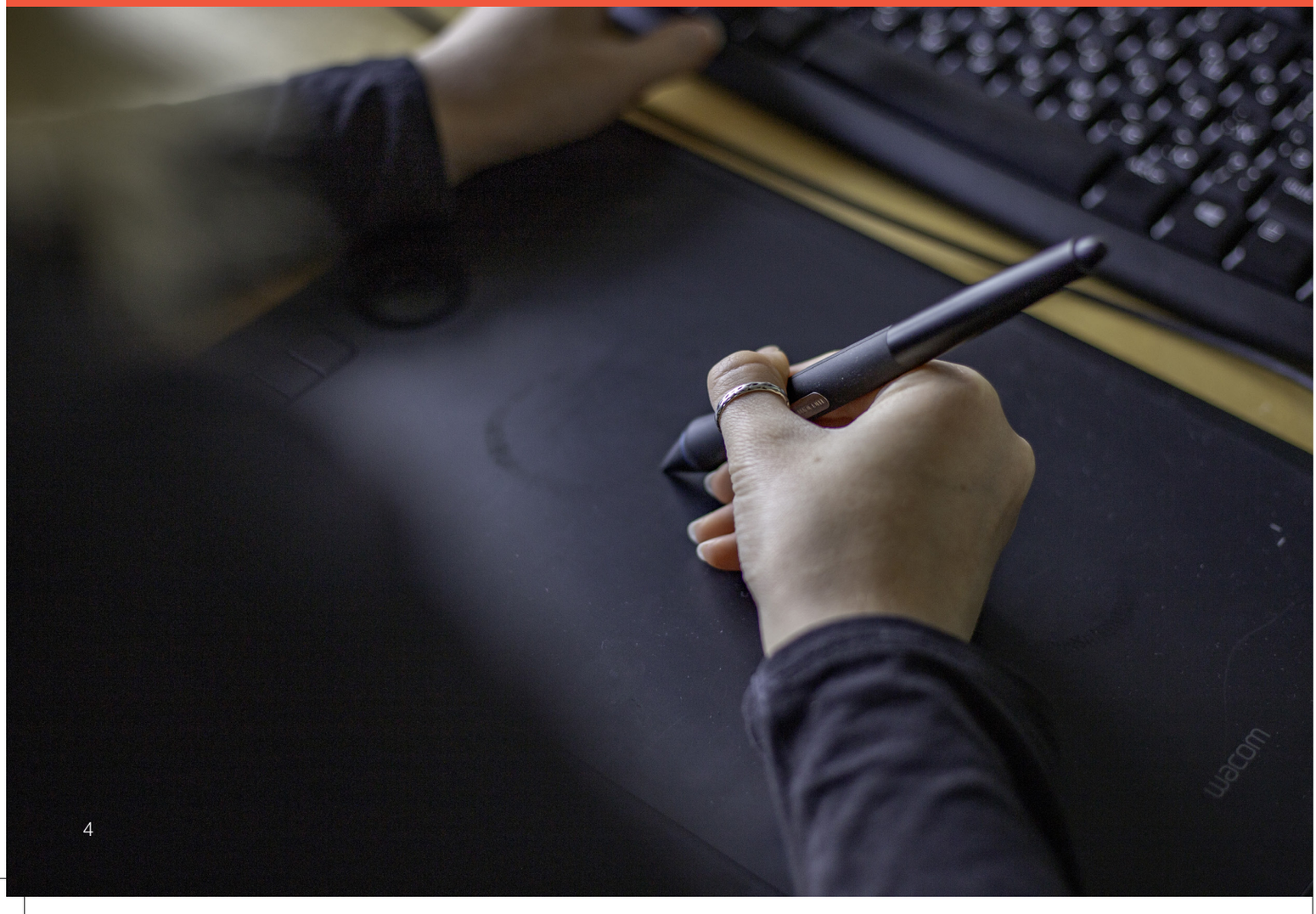
Obsah

Úvod

Zrychlující se adopce cloudových služeb, migrace tradičních datových center do cloudu a stavba nových řešení s přístupem „cloud first“ už teď vede k diskuzím na témata, která ještě před pár lety byla akademická nebo založená pouze na odhadech a předpokladech.

Zatímco odpovědi na technologické otázky výhod a úskalí přechodu ke cloudovým službám se začínají velmi čitelně rýsovat již teď a volby mezi „infrastructure as a service“, „platform as a service“ a „software as a service“ už probíhají na racionální půdě empiricky ověřených důkazů, kybernetická bezpečnost připomíná Pandořinu skříňku. Tajemnou, zavřenou a opředenou strachem z otevření, třeba i jen přímo položenou otázkou.

Rozhodli jsme se nahradit předsudky a mýty fakty a zeptat se.

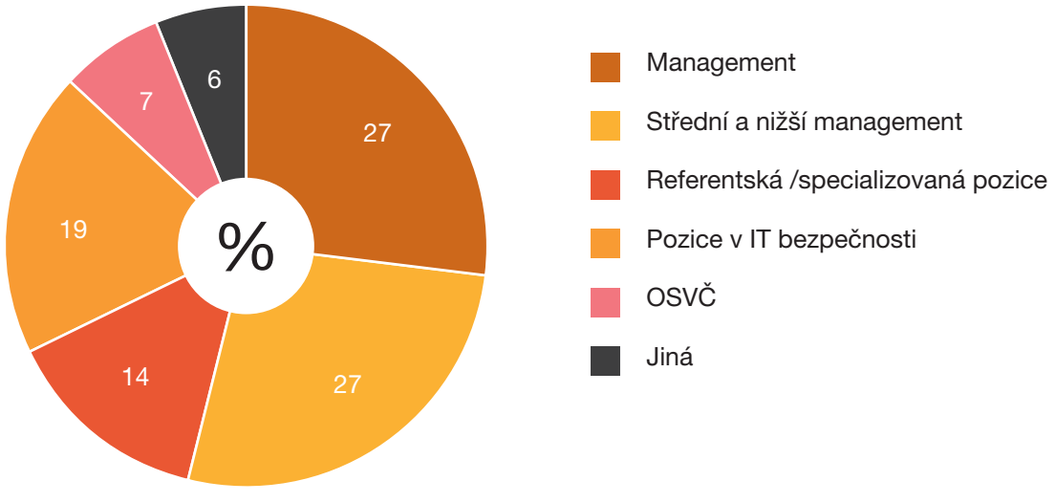


O průzkumu

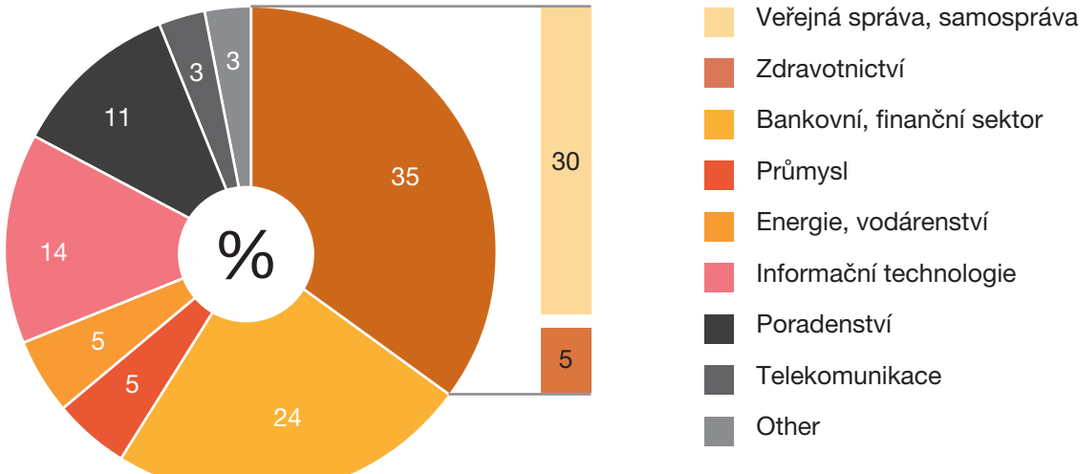
Společnost PwC připravila ve spolupráci s TATE International průzkum s názvem Bezpečnost cloudu ve veřejné a soukromé sféře. Cílem průzkumu bylo zjistit, jak respondenti vnímají bezpečnostní rizika a výhody cloudových služeb oproti tradiční (on-premise) infrastruktuře. Mezi další cíle patřilo prozkoumat, do jaké míry organizace využívají, popř. plánují využívat, cloudové služby, jaké mají nasazené kontroly, a zda využívají standardy specializující se na cloud computing.

Data byla sesbírána během tří příležitostí – Akademie ICT Managementu organizovaná TATE International, Letního Soirée pořádaného stejnou organizací a Business Continuity Fóra organizovaného PwC. Majoritní cílovou skupinou byli manažeři. Dotazníkového šetření se zúčastnilo celkem 102 osob. Respondenti pocházeli z různých oblastí soukromého a veřejného sektoru, přičemž 55 % z nich pracovala na manažerské pozici.

Pozice



Sektory

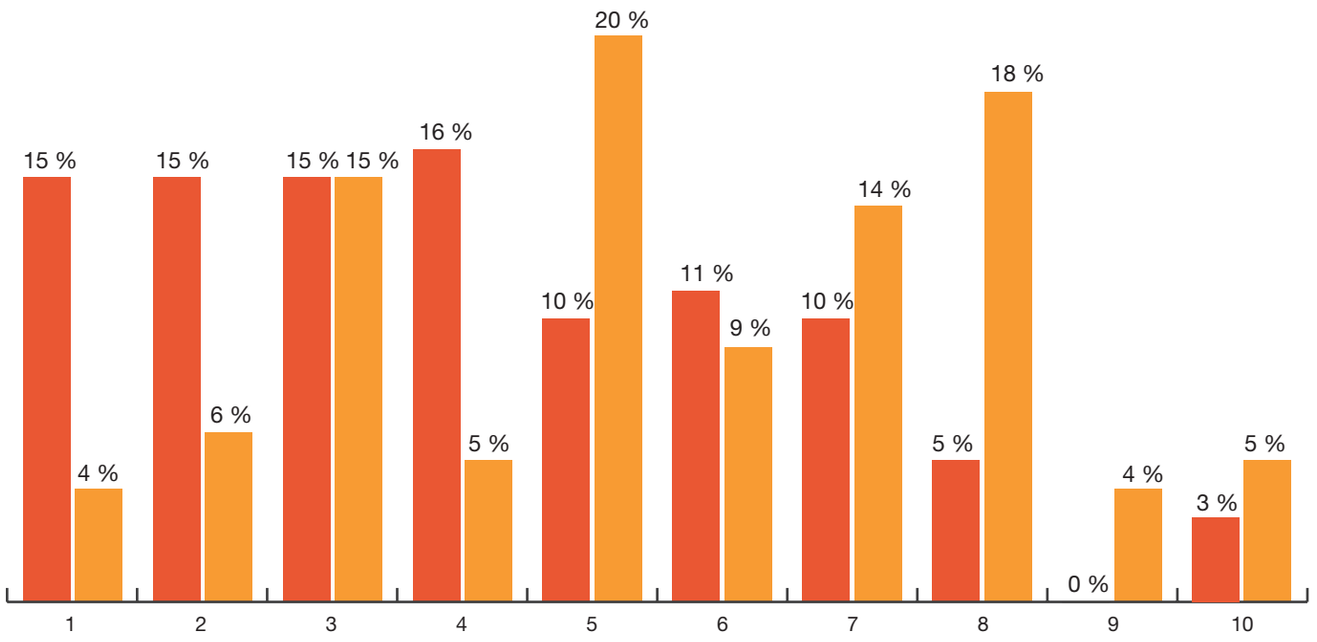


Governance

Aktuální vs. plánované využívání cloudových služeb

Do jaké míry vaše organizace používá cloudové služby?

Jaký je dlouhodobý cíl vaší organizace ve využívání cloudových služeb?



1 - žádná cloudová služba

10 - pouze cloudové služby

Využití cloudových služeb v organizacích nelze považovat za zanedbatelné

Momentálně převládá využívání tradiční on-premise infrastruktury

Pouhých 25% organizací ovšem plánuje pokračovat v majoritním využívání tradiční infrastruktury

27% organizací plánuje využívat především cloudové služby

4,1

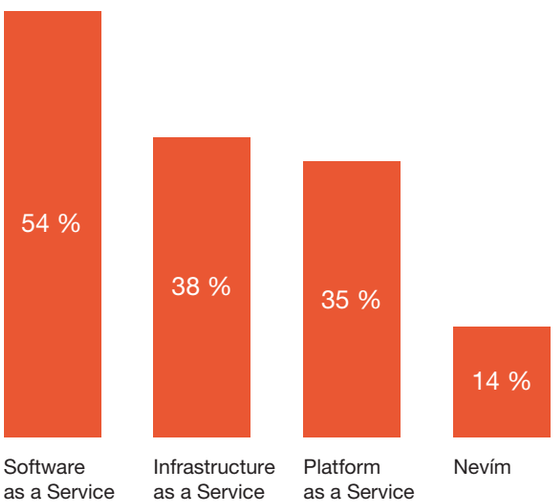
Průměrné hodnoty
Aktuální vs. plánované využití

5,6

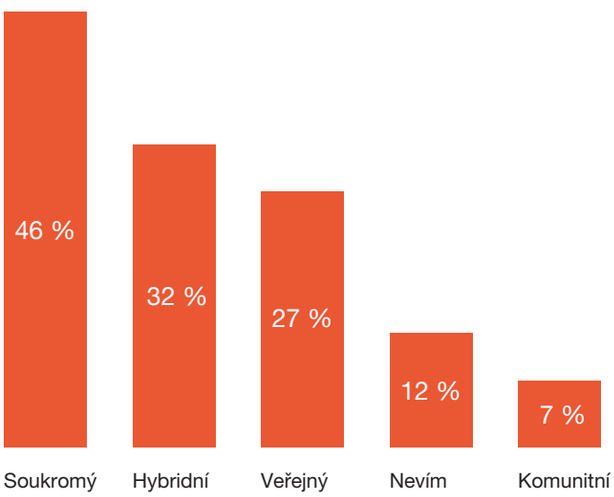
Do budoucna lze pozorovat trend zapojování více cloudových služeb

Druhy využívaných cloudových služeb

Z pohledu distribučního modelu



Z pohledu modelu nasazení



14 %

resp. 12 % respondentů neví, jaký typ cloudu používá

Distribuční model

Určuje jaké komponenty (HW, SW) jsou doručovány v rámci služby

Infrastructure as a Service (IaaS)
- Poskytovatel dodává IT infrastrukturu
- Např. úložiště, servery, síťové komponenty, virtualizace
- Zákazník nasazuje vlastní operační systém a aplikace

Platform as a Service (PaaS)
- Poskytovatel dodává IaaS + operační systém, middleware, knihovny pro vývojáře a další
- Zákazník nasazuje vlastní aplikace

Software as a Service (SaaS)
- Poskytovatel dodává PaaS + aplikace, nástroje, správu dat

Model nasazení

Určuje jakým způsobem a komu jsou služby doručovány

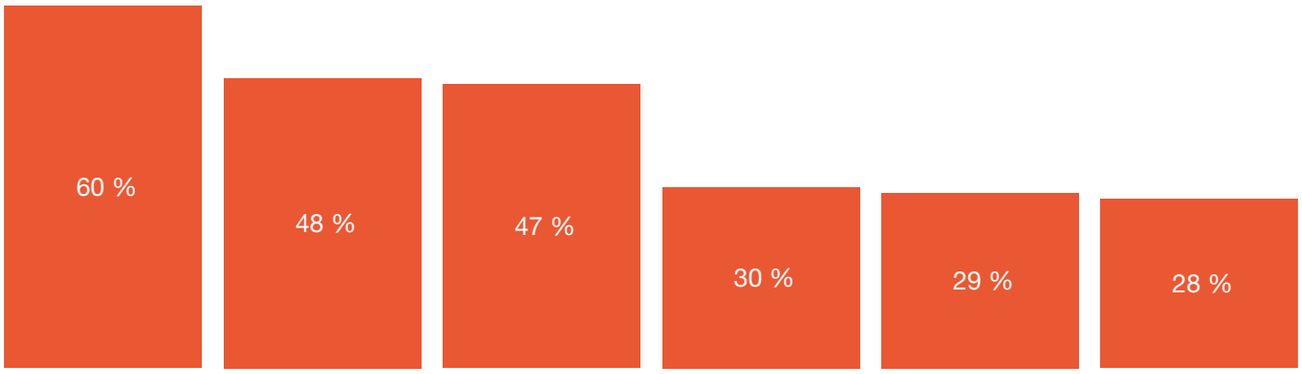
Veřejný cloud
- Nejčastější typ cloudu
- Poskytován veřejnosti

Soukromý cloud
- Cloud dedikován pouze pro určitého zákazníka
- Využíván z bezpečnostních důvodů

Komunitní cloud
- Využíván určitou skupinou subjektů sdílející určité zájmy/cíle

Hybridní cloud
- Kombinace dvou a více typů cloudu
- V posledních letech roste jeho využití

Z pohledu konkrétních druhů služeb/aplikací



Další odpovědi:
Nástroje pro IT služby (např. administrace, help desk) (22%), Cloud nevyužívám(e)/nedokážu/nechci odpovědět (10%), Bezpečnostní nástroje (6%), Ostatní (4%)

Uživatelé využívají cloudové služby mnohem více, než si sami myslí.
Při využívání osobních emailů, internetových úložišť, kalendářů, různých dalších on-line nástrojů – ve všech těchto případech využívají právě cloudové služby.

Co PwC a cloudové platformy?

Jako hlavní cloudovou platformu má PwC nasazeno Google Apps. Zaměstnanci zde mohou využívat služby, jako jsou Gmail, Google Drive, Hangouts, Meet, Calendar, Vault, Google Docs, Google Sheets, Google Slides a další. PwC využívá také cloudové služby Microsoftu (např. Azure, Power BI).

Vedle toho má PwC nasazeny také další cloudové služby – např. Salesforce (CRM systém).

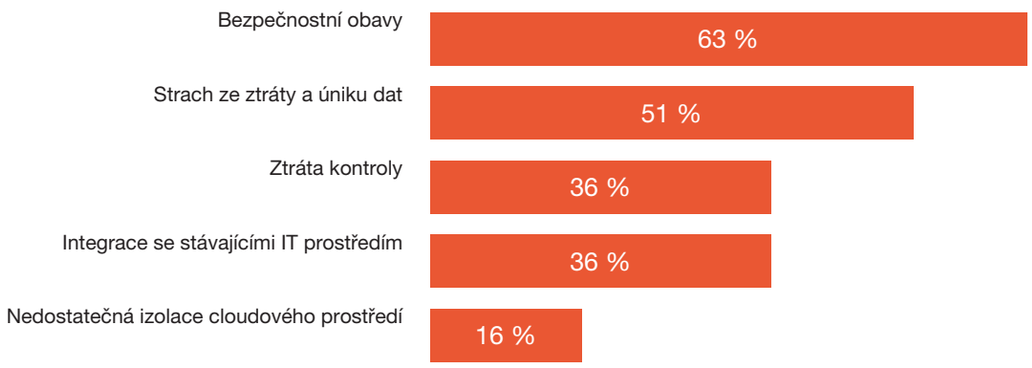
A co další široce používané cloudové platformy?

Mezi ně patří zejména Office 365, který poskytuje podobný balík služeb jako Google Apps. Jednotlivé služby jsou zde napojeny na aplikace Microsoft Office, jako je např. Word online, Excel online a PowerPoint online.

Zákazníci si často pronajímají výpočetní výkon od cloudových poskytovatelů. Nejčastějšími platformami nabízející výpočetní zdroje jsou Google Cloud Platform, Microsoft Azure, Amazon Web Services a IBM Bluemix.

Bariéry adaptace cloudových služeb

S jakými omezeními a bariérami adaptace cloudových služeb musí organizace/uživatelé počítat?



Další odpovědi:
Omezený monitoring a logování (12%), Cloud nevyužívám(e)/nedokážu/nechci odpovědět (11%), Výkonnostní omezení (6%), Ostatní (1%)

Adaptace cloudových služeb

Organizačně významná transformace
Transformace má svoje fáze a pravidla

PwC využívaný rámec transformace - PwC Transformation Strategy Framework

- Aplikovaný na libovolnou změnu v IT
- Od strategie až po provoz
- Vytvořen na základě good practice

Nad všemi fázemi jsou aktivity:

- Programme management office
- Change management

Jednotlivé fáze - PwC Transformation Strategy Framework:

- Strategy & Assess
- Design
- Construct
- Implement
- Operate & Review

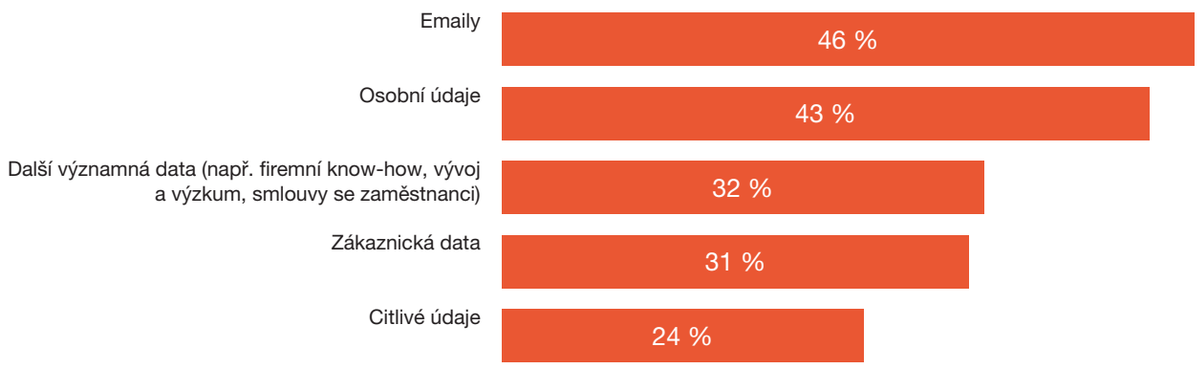
Mezi všemi fázemi je kontrola kvality a hodnocení správného směřování transformace
Více informací v závěru tohoto reportu.

Transformace na cloudové služby je obzvláště náročným procesem, jelikož se mění celkový způsob využívání IT prostředků v organizacích.

Přechází se od lokálních výpočetních komponent k integraci komponent, které jsou umístěné mimo organizaci a které nejsou pod její výhradní kontrolou. S tím přichází i požadavky na změnu smluv, politik, procedur, řízení ochrany dat, kontrol, bezpečnostního nastavení a plno dalšího.

Uchovávaná data v cloudu

Jaké druhy dat organizace v cloudu uchovávají?



Další odpovědi:
Cloud nevyužívám(e)/nedokážu/nechci odpovědět (16%), Ostatní (9%), Zdravotní záznamy (3%)

Pohled uživatele cloudové služby

- Posílá emaily s osobními a citlivými daty
- Sdílí fotky na Facebooku a Instagramu
- Využívá Dropbox, Google Drive nebo OneDrive k ukládání souborů
- Používá aplikaci pro ukládání hesel (příp. i čísel kreditních karet)
- Posílá partnerovi fotografie přes mobilní aplikaci (i intimní)
- Přeposílá si firemní věci na svůj email/ukládá na svoje internetové úložiště

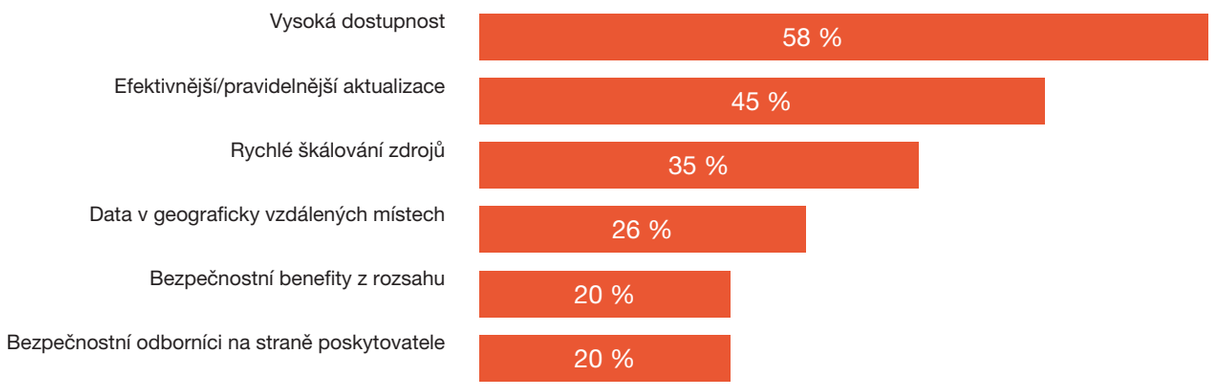
Je důležité si uvědomit, že uživatel téměř nikdy neví:

- kde jsou jeho data uložena
- kolik jejich kopií existuje
- jak jsou data zabezpečena
- jak je pro útočníka jednoduché/náročné napadnout poskytovatele služby a data ukrást
- jaké jsou právní nároky států, u nichž jsou data uložena

Bezpečnost, rizika

Bezpečnostní výhody cloudových služeb

Jaké bezpečnostní výhody přináší cloudové služby organizacím?



Další odpovědi:
Silné bezpečnostní prvky – reputace poskytovatelů je závislá na bezpečnosti jejich služeb (15%), Cloud nevyužívám(e)/nedokážu/nechci odpovědět (12%), Izolace aplikací a sítí (6%), Ostatní (3%)

47 %

Aktualizace, záplatování

Tyto procesy bývají běžně podřízeny provozním a byznysovým prioritám a musí se vejít do určitých udržovacích oken. V případě cloudových služeb se zákazníci o tyto procesy nestarají, jelikož jsou prováděny na straně poskytovatele.

Rychlé škálování zdrojů

Cloudové služby umožňují zákazníkům, aby během okamžiku získali více výpočetního výkonu. Z hlediska bezpečnosti to může být zautomatizováno např. pro případ útoku typu Denial of Service.

35 %

26 %

Data v geograficky vzdálených místech

Data bývají ukládána ve více kopiích umístěných v geograficky vzdálených datových centrech. V případě poruchy jednoho centra (např. z důvodu živelné katastrofy) a zničení všech dat v něj umístěných, nedojde k celkové ztrátě dat, jelikož jejich kopie jsou uloženy v jiných datových centrech.

Bezpečnostní benefity z rozsahu, bezpečnostní odborníci

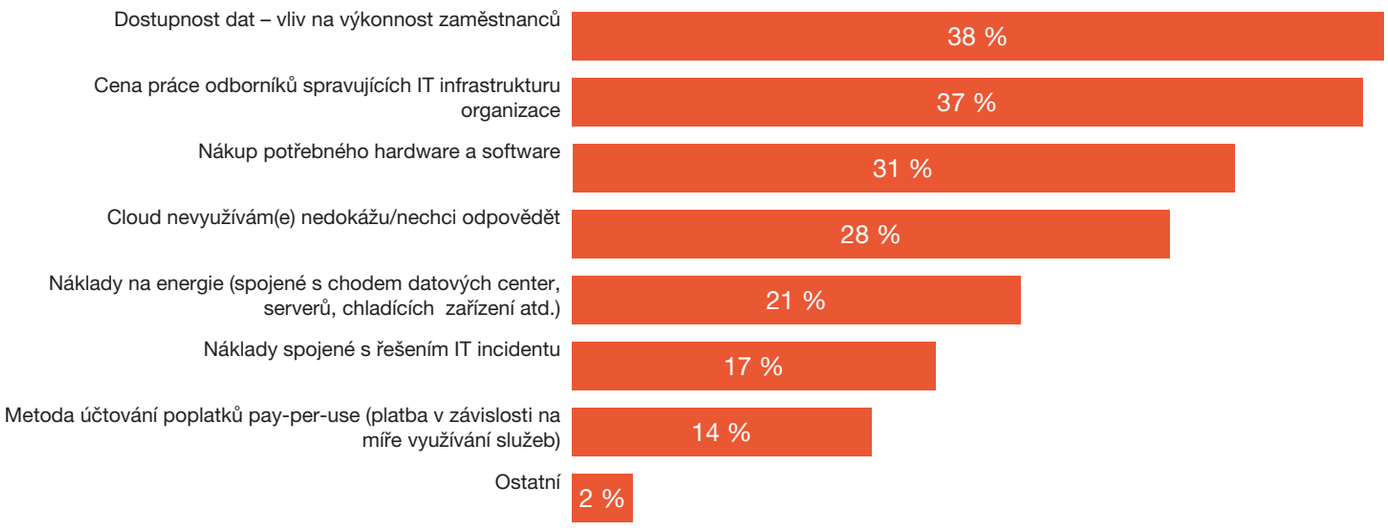
Poskytovatelé cloudových služeb mají zabezpečení nabízených produktů na vyšší úrovni než zabezpečení IT prostředků u běžných organizací. Zároveň zaměstnávají zpravidla větší množství bezpečnostních expertů, kteří se přímo starají o zabezpečení služeb.

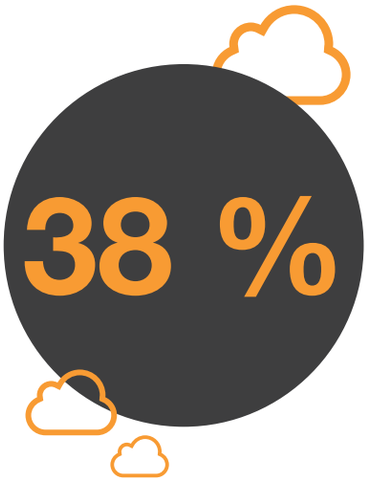
20 %

Poskytovatelé cloudových služeb vnímají propojení úrovně bezpečnosti služeb s jejich reputací, což je přímo typické pro poskytovatele nehmotných služeb.

Finanční úspory cloudových služeb

V jakých oblastech vidí organizace největší úspory při využití cloudových služeb?





Vysoká dostupnost ovlivňuje chod cloudových služeb. Jejich bezproblémový chod je závislý na kvalitě datových center, ve kterých jsou data uchovávána. Datová centra jsou hodnocena podle kvalifikace Tier.

Data Center Tiers (Vrstvy datových center)

Klasifikace infrastruktur datových center
Hodnocena je kvalita systémů, opatření proti vnějším vlivům, zabezpečení a další

Tier 1 – Základní infrastruktura, absence redundantního napájení, chlazení a většiny IT vybavení.
- Dostupnost 99,67 % času – povolený výpadek 28,8 h za rok.

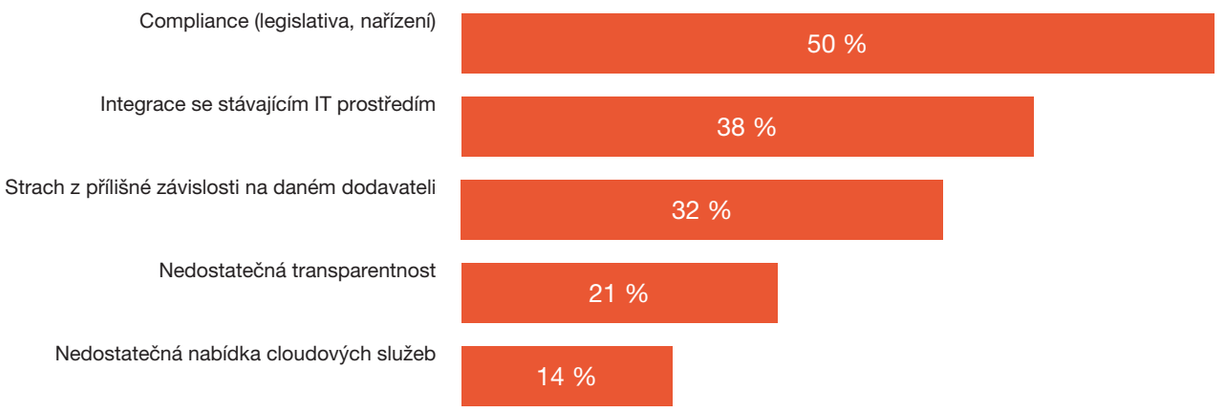
Tier 2 – Přidává redundanci vybraných prvků (nikoli napájení a chlazení).
- Dostupnost 99,74 % času – povolený výpadek 22 h za rok.

Tier 3 – Přidává redundanci napájení, chlazení a dalších vybraných prvků
- Dostupnost 99,98 % času – povolený výpadek 1,6 h za rok.

Tier 4 - Redundance všech komponent. Výpadek libovolné komponenty datového centra nijak neovlivní chod systémů/služeb (fault tolerance).
- Dostupnost 99,99 % času – povolený výpadek 0,8 h za rok.

Bezpečnostní překážky cloudových služeb

S jakými bezpečnostními překážkami se musí organizace využívající cloudové služby potýkat při jejich používání?



Další odpovědi:
Cloud nevyužívám(e)/nedokážu/nechci odpovědět (14%), Nedostatek znalostí (12%), Finance (12%), Nedostatečné přizpůsobení cloudových služeb (12%), Dostupnost (7%), Ostatní (2%)

Jaké jsou naše zkušenosti? Jaké jsou hlavní problémy našich klientů?

V současné má době mnoho organizací obavy z **regulatoriky outsourcingu**, která se týká také cloudových služeb.

Regulovaný je zejména **finanční sektor** a kritická infrastruktura státu.

Častým problémem integrace cloudových služeb je **řízení identity**, konkrétně federace identity mezi cloudovými službami a systémy našich klientů.

Zákazníci cloudových služeb musí mít dostatečnou míru jistoty v **poskytovateli** služeb, jelikož ochranu dat nemají pod svojí výhradní kontrolou.

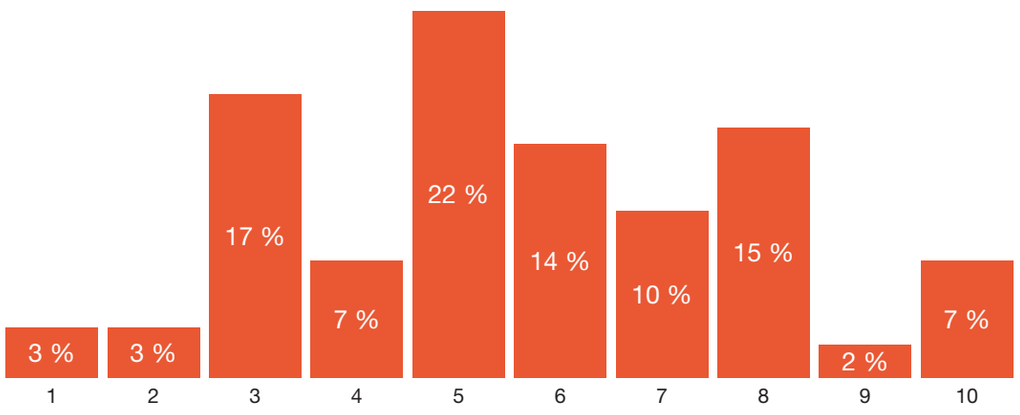
Federace identit, Identity as a Service

Federace identit je princip, který zákazníkům umožňuje, aby jejich zaměstnanci mohli přistupovat ke cloudovým službám na základě přihlašovacích údajů do interních systémů.

Federace identit je běžnou součástí typu služeb, známých jako Identity as a Service, které organizacím nabízejí nástroje a možnosti k řízení identit. Běžnou součástí Identity as a Service je princip Single Sign-On, tedy jednotné přihlášení do všech systémů v organizaci, včetně využívaných cloudových služeb.

Bezpečnostní rizika – tradiční řešení vs cloudové služby

Jsou bezpečnostní rizika více spojena s cloudovými službami, nebo s tradičním on-premise řešením?



1 – tradiční infrastruktura
10 – cloudové služby

5,57
Průměrná hodnota z grafu

Organizace připisují bezpečnostní rizika více cloudovým službám. Nejde ovšem o razantní rozdíl.

Základem zhodnocení aktuálního stavu a nastavení správných bezpečnostních kontrol je vždy analýza rizik

Analýza rizik cloudových služeb v porovnání s analýzou rizik tradičních on-premise systémů

Jiné kontroly
- Např. pouze vybraná data posílána do cloudové služby

Jiná opatření
- Např. zavedení pravidel akceptovaného použití cloudových služeb v organizaci

Jiné katalogy hrozeb, zranitelností a aktiv
- Např. publikace Cloud Computing: Benefits, Risks And Recommendations For Information Security od organizace ENISA

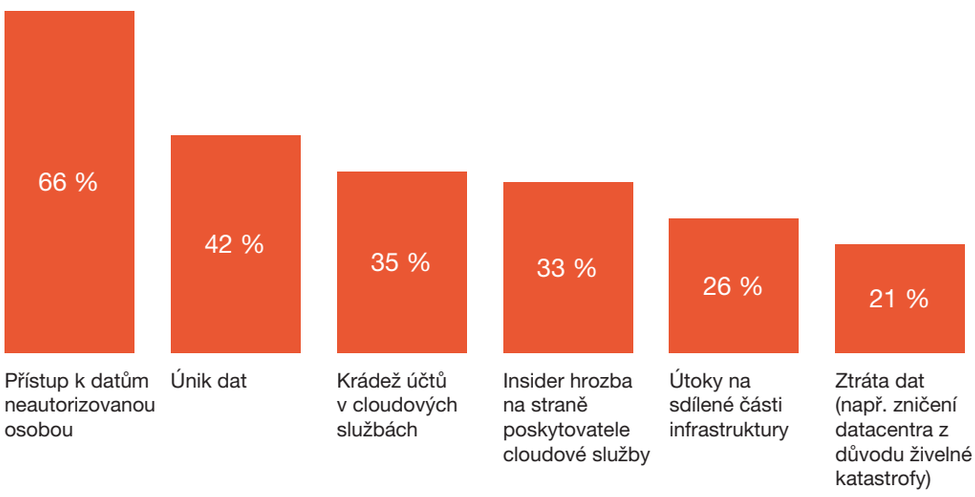
Jiné scénáře rizik
- Publikované také v publikaci uvedené výše od organizace ENISA

Jiný přístup
- Např. potřeba zahrnout i zabezpečení na straně poskytovatele služeb

Další prvky
- Např. zahrnutí speciálních standardů, legislativy, proces migrace

Bezpečnostní hrozby cloudových služeb

Co považují organizace za bezpečnostní hrozby cloudových služeb?



Další odpovědi:
DoS útok (11%), Nasazení malware (10%), Cloud nevyužívám(e)/nedokážu/nechci odpovědět (9%)

Top 12 hrozeb cloud computingu dle organizace Cloud Security Alliance (CSA)

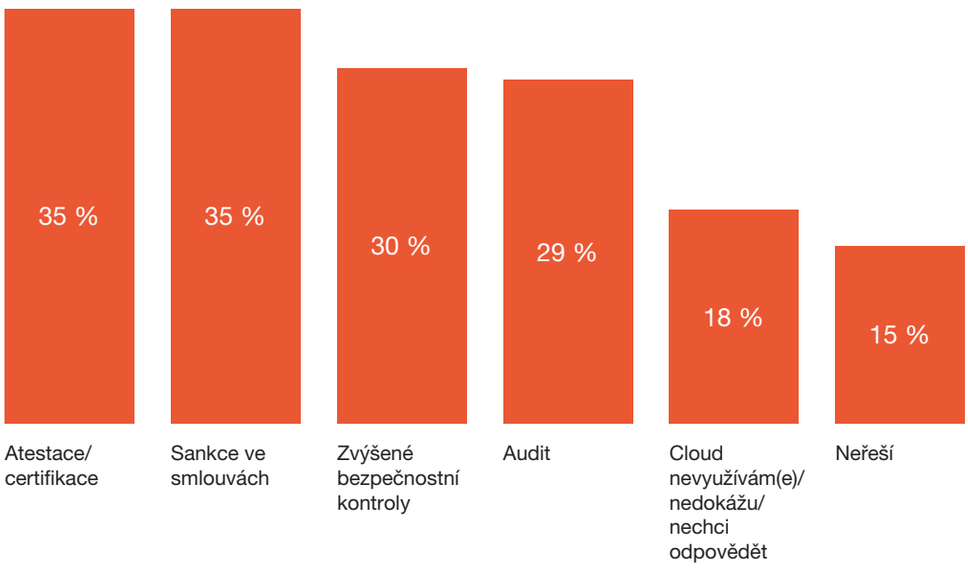
1. Únik dat
2. Nedostatečné řízení identit, přihlašovacích údajů a přístupu
3. Nezabezpečené rozhraní a API
4. Zranitelnosti systému
5. Krádež účtů
6. Insider hrozba
7. Advanced Persistent Threat
8. Ztráta dat
9. Nedostatečné Due Diligence
10. Zneužití, zločinné využití cloudové služby
11. Denial of Service
12. Zranitelnosti sdílených technologií

Zdroj: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Kontroly, bezpečnostní opatření

Zaručení bezpečnosti dat v cloudu

Jak organizace reagují na skutečnost, že na nastavení bezpečnosti cloudových služeb mají vliv poskytovatelé těchto služeb?



Co jednotlivá ujištění znamenají?

Assurance
- obecné ujištění o určitém stavu prostředí, obvykle vydávané ve formě tzv. reasonable nebo negative assurance
- ověřující strana vydává potvrzení, že nic nenasvědčuje tomu, že udávaný stav prostředí neodpovídá skutečnému

Audit
- konkrétní forma ujištění, nejčastěji spojovaná se statutárním (finančním) auditem posuzujícím validitu účetní závěrky
- může jít také o audit podle konkrétního standardu

Atestace
- písemné potvrzení o provedeném testu
- termín, který není v mezinárodních standardech pro audit přesně definován

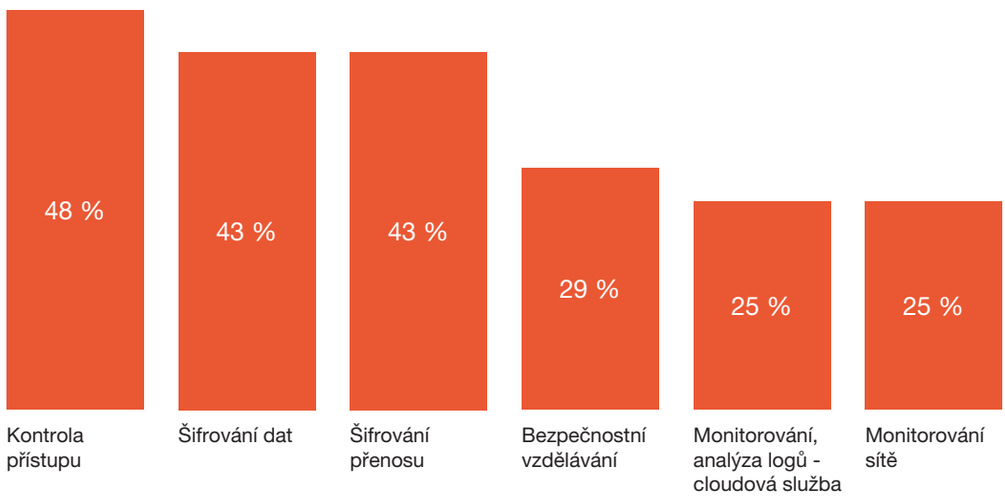
Certifikace
- potvrzení, že současný stav daného prostředí odpovídá zavedenému standardu
- příkladem je rodina standardů ISO/IEC 27000

Ověřovací zakázky SOC (Service Organization Controls)
- představují konkrétní formu ujištění o souladu kontrol u dodavatelských organizací (IT outsourcing)
- se vzrůstajícím číslem typu reportu (SOC 1 až 3) roste míra ujištění o bezpečnosti dodavatele

Akreditace
- forma souhlasu nadřazené strany za účelem umožnění provozování určitého informačního systému (příp. jiného objektu) v daném prostředí

Bezpečnostní kontroly a opatření cloudových služeb

Jaké mají organizace zavedené/plánované bezpečnostní kontroly a opatření cloudových služeb?



Konfigurace bezpečnosti cloudových služeb by měla být samozřejmost

Před samotným používáním cloudových služeb je velice důležitá jejich správná konfigurace, zejména co se týká bezpečnostního nastavení. Tímto krokem se optimalizuje využívání dané služby a zákazníci se chrání před útoky na služby využívající předdefinované iniciální nastavení.

Příklady bezpečnostních konfigurací, které by neměly být opomenuty:

- Nastavit dostatečně silnou autentizaci pro uživatele
- Nastavit vícefaktorovou autentizaci pro administrátory
- Nastavit přístupová práva jednotlivých rolí/uživatelů/skupin
- Nastavit správnou klasifikaci dat a relevantní bezpečnostní opatření

Bezpečnostní incident

Případová studie: Hotelový řetězec – únik dat

Únik dat 600 milionů klientů tohoto hotelového řetězce – jména, čísla kreditních karet, emailové adresy, čísla pasů a další.

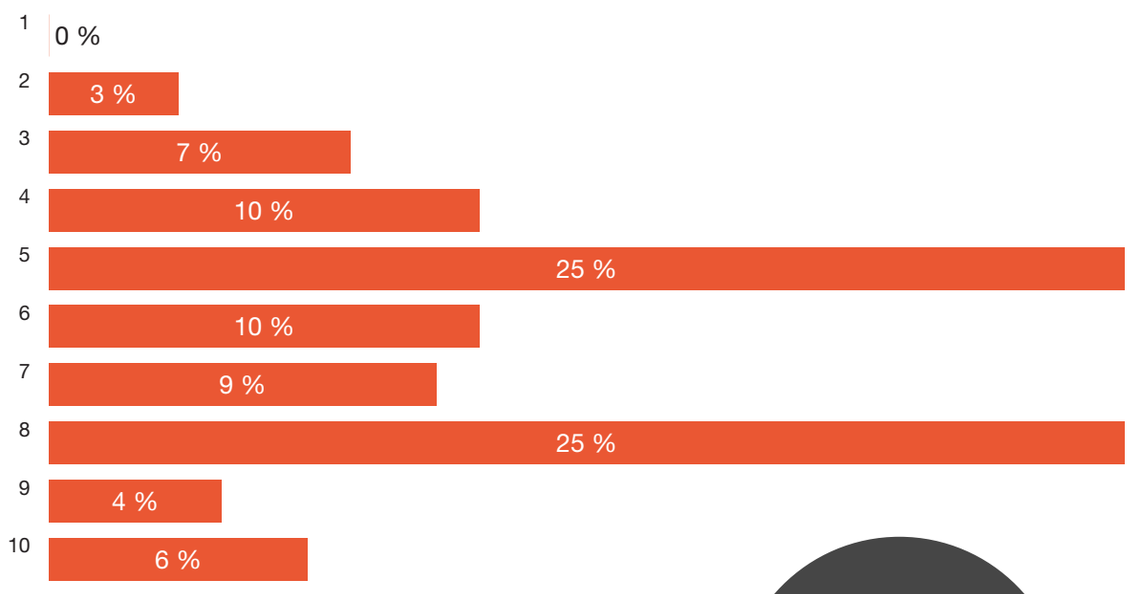
Bezpečnostní nástroje detekovaly neoprávněný přístup do databáze v roce 2019, útočník byl ovšem v systému od roku 2013.

Útočníkům se podařilo nabourat databázi s rezervacemi skrze rezervační systém hotelu, který je volně dostupný na internetu. Vstup do databáze nebyl dostatečně zabezpečen, zároveň nebyla dostatečně monitorována aktivita uvnitř databáze.

Mezi opatření vedoucí ke snížení možného úniku dat patří např. DLP a PAM řešení, threat hunting, kontrola vstupních dat, pravidelné přezkoumání bezpečnostních opatření.

Dostatečnost kontrol a opatření cloudových služeb

Pokud organizace používají cloudové služby, považují zavedené bezpečnostní kontroly a opatření těchto služeb za dostatečné?



1 – Nedostatečné
10 – Dostatečné

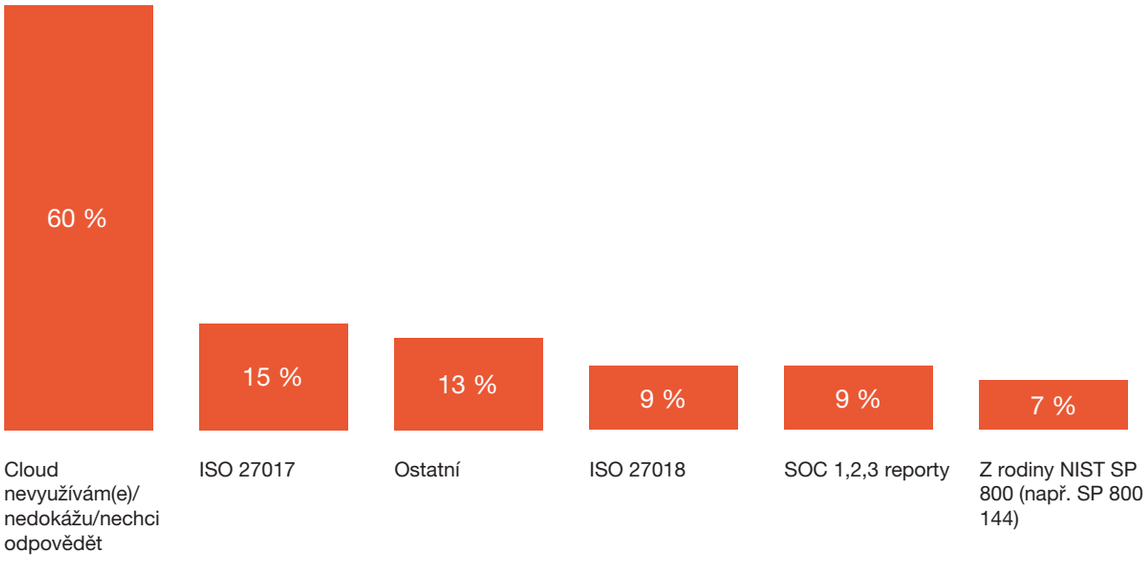
5,56
Průměrná hodnota

Ochrana soukromí

Ochrana soukromí a zajištění souladu s regulacemi, jako je GDPR, se stává standardem a nedílnou součástí strategie cloudové bezpečnosti. Umístění datových center mimo EU s sebou nese povinnost implementace dalších opatření. Počet společností, kterým se nepodařilo veškerá opatření plně implementovat, zobrazuje následující graf.

Bezpečnostní standardy cloudových služeb

Jaké standardy, specializující se na cloud computing, jsou v organizacích využívány?



Příklad bezpečnostních standardů, kontrol

- **Rodina standardů ISO/IEC 27000** – Bezpečnostní standardy vydávané organizací International Organization for Standardization, která působí zejména na území Evropy.
- **Rodina standardů NIST SP 800** – Bezpečnostní standardy využívané zejména v USA. Standardy navázány na americkou legislativu.

- **ISO/IEC 27017** – Rozšíření bezpečnostního standardu ISO/IEC 27002 o specifika cloudových služeb. Zahrnuje kontroly poskytovatele i uživatele cloudové služby.
- **ISO/IEC 27018** – Rozšíření bezpečnostního standardu ISO/IEC 27002. Zaměřuje se na ochranu osobně identifikovatelných informací ve veřejných cloudech.

- **SOC 1 report** - Interní kontrola finančního reportingu, za účelem auditu finančních výkazů, interní report.
- **SOC 2 report** - Kontrola IT prostředí, bezpečnosti dat, zpracování dat, interní report.
- **SOC 3 report** - Kontrola IT prostředí, bezpečnosti dat, zpracování dat, report určen pro veřejnost.

Veřejně dostupné informace o shodě s bezpečnostními standardy

Některé organizace poskytují veřejné informace o shodě s různými standardy, legislativními nařízeními a dalšími.

Např. Amazon Web Services (AWS) - https://aws.amazon.com/compliance/programs/

Služby PwC

Nabídka služeb PwC

PwC Transformační rámec

Strategie & analýza

- Analýza rizik informační bezpečnosti, hodnocení aktuálních organizačních a technických opatření na straně uživatele i poskytovatele cloudové služby
- Benchmarking (srovnání s ostatními organizacemi)
- Identifikace nedostatků k odstranění/oblastí ke zlepšení souvisejících s cloudovými službami
- Posouzení shody s normami ISO/IEC 27017, 27018
- Definice cílových bezpečnostně-provozních modelů
- Definice přechodných plánů, harmonogramů a podpora prioritních obchodních případů

Návrh

- Návrh možných řešení, opatření a procesů zabezpečení cloudu
- Identifikace klíčových cloudových služeb pro náběh
- Vypracování podrobného plánu přechodného období
- Výběr poskytovatele cloudových služeb (podpora v procesu RFI/RFP)

Vývoj

- Zajištění cloudových bezpečnostních procesů, nástrojů, rámců, politik a dalších dílčích výstupů podporujících cloudové řešení
- Zajištění životního cyklu vývoje zabezpečení v cloudu (jak Agile, tak i Waterfall)
- Přehled architektury zabezpečení ve vztahu ke cloudovým službám
- Hodnocení bezpečnosti poskytovatelů cloudových služeb a smluv (tj. náležitá péče)

Implementace

- Implementace cloudových bezpečnostních procesů, nástrojů, frameworků, politi a dalších výstupů do firemního prostředí
- Implementace správy cloudových služeb
- Poskytování školení managementu a workshopů pro pochopení specifik zabezpečení cloudu
- Zajištění kvality při náběhu a zajištění hladkého přechodného období
- Den 1 připravenost k implementaci cloudu (formou „dryrun“, „tabletop“ nebo funkční připravenost)

Provoz & přezkoumání

- Průběžné monitorování zabezpečení cloudu a integrace do SOCu
- Pravidelný bezpečnostní audit, hodnocení zranitelností a bezpečnostní architektury
- Poradenství v oblasti řešení správy identit v cloudu (důvěra v digitální identitu, federace)
- Poskytování reportů pro správu, které podporují rozhodnutí vrcholného managementu v oblasti zabezpečení cloudu
- Nastavení kroků a akcí souvisejících s cloudovými službami pro zajištění kontinuity provozu
- Zapojení forenzního oddělení v případě vyšetřování
- Posouzení IT prostředí/cloudových služeb za účelem poskytnutí SOC2 zprávy

Aplikovatelné pro všechny fáze Transformačního rámce:

1 Projektová kancelář
Poskytování odborných znalostí v oblasti IT Projektový management

2 Řízení změn
Řízení všech změn v rámci společnosti souvisejících s přechodem zabezpečení cloudu

3 QA / Atestace
Včetně provedení nezávislého atestu či provedení postupů dle konkrétního auditorského standardu

Poděkování

V první řadě chci poděkovat všem, kteří nám pomohli svými odpověďmi na naše otázky. Bez vás by náš průzkum měl jen velmi omezená nebo i žádná data a naše závěry by zůstaly v rovině dohadů a spekulací.

Spolupráce s TATE International pak byla potěšením, a je nám ctí poděkovat za podporu, bez které by tento průzkum pravděpodobně vůbec nevznikl.

A v poslední, ale neméně důležité, řadě, chceme poděkovat všem Vám, kteří jste dočetli až sem – a doufáme, že šlo o čas zajímavě a užitečně strávený. Váš zájem o kybernetickou bezpečnost je nadějí pro bezpečnost naší společnosti a pro rozvoj našeho odvětví jako takového.

Neváhejte nás kontaktovat

Petr Špiřík

Petr je ředitelem oddělení Cyber & Privacy a má za sebou více než 15 let praxe v informační a kybernetické bezpečnosti. Petr vedl řadu týmů v globální struktuře PwC a také zastával funkci regionálního CISO.

petr.spirik@pwc.com
+420 774 191 101

Michal Wojnar

Michal vede v rámci oddělení Cyber & Privacy tým konzultantů zaměřených na informační bezpečnost, ochranu osobních údajů a krizové řízení. Michal má za sebou více než 9 let praxe a řadu úspěšných projektů.

michal.wojnar@pwc.com
+420 724 726 166

Michal Čábela

Michal vede v rámci oddělení Cyber & Privacy tým Cyber Resilience. Má více než 10 let zkušeností v oblasti kybernetické bezpečnosti a zaměřuje se na oblasti Enterpise Architecture, OT/ICS Security a vývoj simulačních nástrojů.

michal.cabela@pwc.com
+420 775 214 115

Martin Zbořil

Martin pracuje jako konzultant v oddělení Cyber & Privacy. Věnuje se oblasti kybernetické bezpečnosti z technického i procesního pohledu. V rámci doktorského studia se věnuje cloudové bezpečnosti.

martin.zboril@pwc.com
+420 734 783 921