Riziká spojené s cloudovými službami vo verejnom sektore

december 2022



www.pwc.com/sk

Riziká spojené s cloudovými službami vo verejnom sektore - agenda

1

Čo je potrebné zvážiť hneď na začiatku

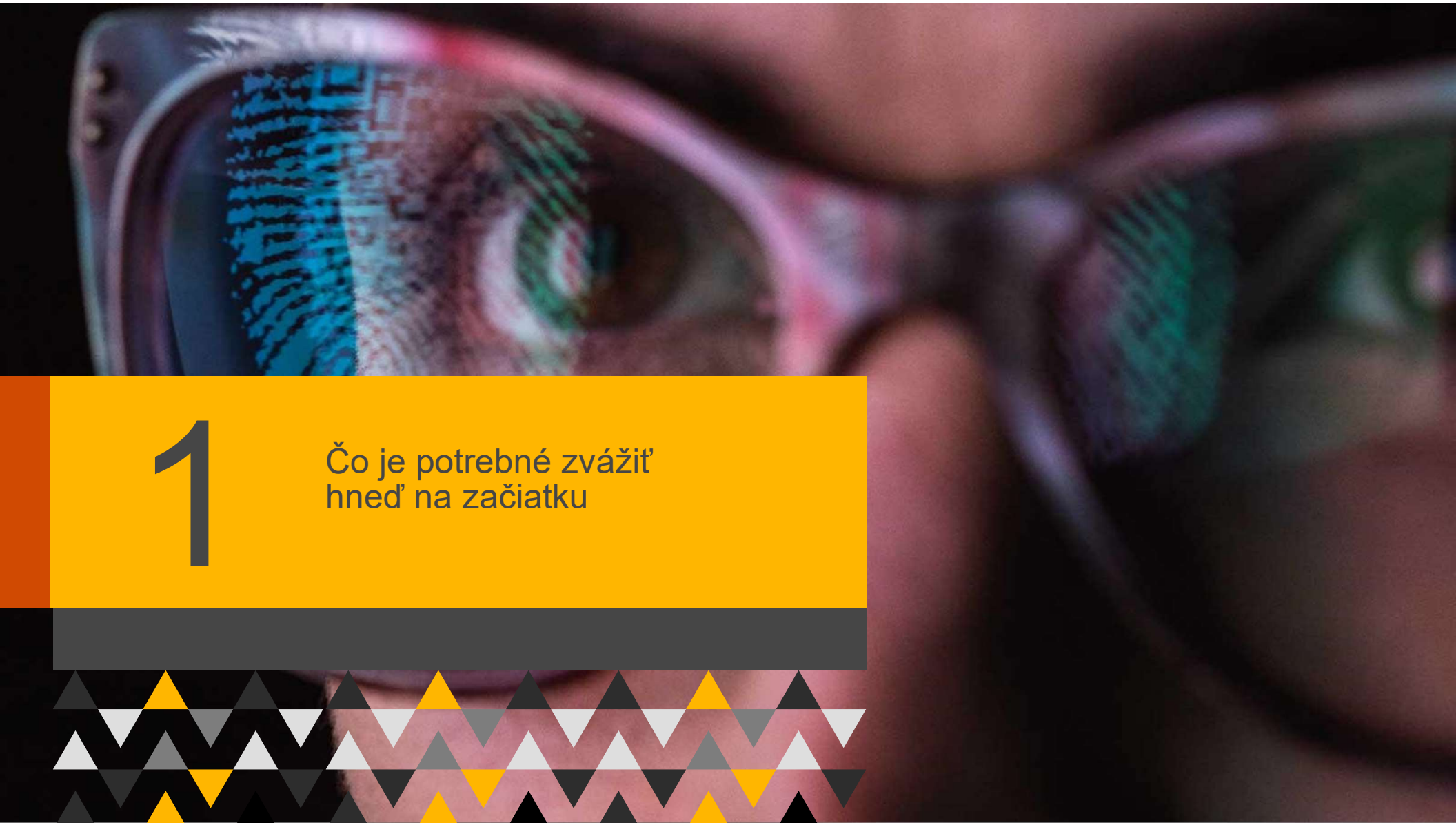
2

1. Príklad identifikovaných rizík na projekte pre verejný sektor

3

2. Príklad identifikovaných rizík na projekte pre verejný sektor





1 Čo je potrebné zvážiť hneď na začiatku

Čo je potrebné zvážiť hneď na začiatku

V súčasnosti mnohé verejne inštitúcie uvažujú nad presunom svojich služieb do Cloud riešení

Čo je však potrebné zvážiť pred samotným rozhodnutím použitia Cloud služieb?

Prvé otázky: Je mi to treba? Prečo by som to mal chcieť?
Časté odpovede: "Je to moderné", "je to IN", "je to v súlade s národnou stratégiou v oblasti IT" a podobne

Čo zvážiť hneď na začiatku:

- Aké mám mať z toho výhody/benefity?
- Aké sú nevýhody?
- Čo vlastne chcem presunúť? (Aké služby (aplikácie), Aké dáta, Všetko alebo len niečo?, Hneď/naraz, alebo postupne?)
- Čo ma to bude stáť?
- Aké **riziká** to obnáša?



Čo je potrebné zvážiť hneď na začiatku - vybrané riziká

"The physical location of the organization no longer defines the security perimeter."

Vybrané kategórie rizík pre cloudové technológie:

- **Identify and access management** - prístupy a oprávnenia nie sú dostatočne a primerane riadené (obmedzené)
- **Third party management -** riziko narušenia kontinuity služieb, resp. výpadok služieb, porušenie ochrany alebo strada údajov
- **Compliance (Legislatíva a regulácie)** - nesúlad s externými a internými predpismi a reguláciami (ZoKB, GDPR, EBA/SBA, …)
- **Incident Response, Notification and Remediation -** nedostatočný monitoring a riešenie prevádzkových a bezpečnostných incidentov
- **Threat and Vulnerability Management -** zraniteľnosti nie sú dostatočne identifikované a odstraňované
- **Portability and interoperability -** nekompatibilita starších systémov s novými (modernými) cloudovými technológiami
- **Business Continuity & EXIT scenarios -** chýbajúce alebo nedostatočne definované procesy zachovania kontinuity alebo EXIT postupov
- **Service contract & SLA -** nedostatočne definovaná úroveň poskytovaných služieb, zodpovedností, garancií a vynútiteľnosti



Čo je potrebné zvážiť hneď na začiatku - Cloud a zdieľaná zodpovednosť





2

1. Príklad identifikovaných rizík na projekte pre verejný sektor

1.príklad

O projekte:

Klientove zadanie bolo vytvorenie systému na tvorbu zmlúv, ktoré sú vytvárané medzi Klientom a druhou zmluvnou stranou.

Zadanie klienta bolo vytvoriť systém, ktorý prevedie zadávateľa ako aj všetkých užívateľov systému celým životným cyklom dokumentu od zadania požiadavky vytvorenia zmluvy, cez pripomienkovací proces až po právne pripomienkovanie a schválenie.

Nový systém zastrešuje kompletný proces vrátane histórie zmien, notifikácií, autorizácií a zdieľania dokumentov.

Použitá technológia:

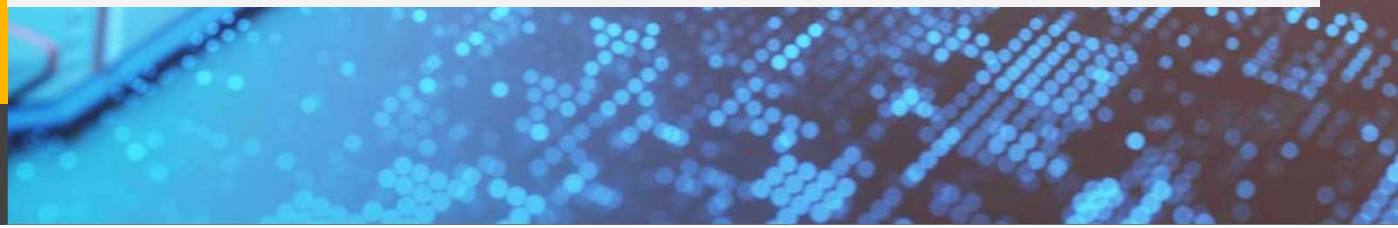
Systém bol vyvinutý na platforme Power Platform. Použité komponenty boli: Power App, Power Automate a Dataverse.

Implementačné výzvy a identifikované kybernetické riziká:

Najväčšou výzvou implementácie bolo zjednotiť historicky zaužívané zvyky a úlohy do jednotného procesu. Zo začiatku bol vytvorený rýchly prototyp, ktorý mohli užívatelia otestovať aby sa potvrdilo, že navrhnutý proces bude použiteľný. Vytvorený systém bol po nasadení intuitívny a menej ako 2% užívateľov potrebovalo pomoc s používaním.

Prístup k Power Platforme - systém je otvorený pre všetkých. Obsah zmlúv je verejný. Dôležitou súčasťou sú obmedzené prístupové práva na editáciu zmlúv a príloh iba pre užívateľov, ktorí boli vybraní do procesu pripomienkovania.

Bol potrebný súlad s legislatívou, hlavne s GDPR a ten bol zabezpečený anomymizáciou dát v rámci procesu pripomienkovania.





3

2. Príklad identifikovaných rizík na projekte pre verejný sektor

2.príklad

O projekte:

CRMP (Cyber Risk Management Platform) slúži na manažment a identifikáciu potenciálnych kybernetických rizík Klienta.

Riešenie stavia už na existujúcej možnosti nahlasovania kybernetického rizika.

Hlavným cieľom platformy je identifikovať potenciálne kybernetické hrozby Klienta, určiť ich dopad a akčný plán na ich odstránenie.

Použitá technológia:

Power Platform (Power Apps, Power Automate, Power BI, Dataverse), SQL, Azure Functions a Azure Data Factory

Implementačné výzvy a identifikované kybernetické riziká:

Ide o vývoj komplexnej aplikácie v cloudovom prostredí s využitím rôznych cloudových služieb.

Bolo potrebné zabezpečiť súlad s EU legislatívou, hlavne s GDPR.

Klient požadoval uchovávanie dát iba v rámci EU.

Vznikla nekompatibilita starších systémov s novými (modernými) cloudovými technológiami, a hľadali sa možnosti migrácie dát.

Prístupy k platforme neboli dostatočne riadené a vznikla potreba zadefinovať proces riadenia prístupov.

Dostupnosť a obstarávanie licencí bol časovo náročný proces.



Kontakty



Martin Srnka
Riaditeľ

+421 902 953 854
martin.srnka@pwc.com



Peter Fridrich
Manažér

+421 918 149 571
peter.fridrich@pwc.com

Ďakujem za pozornosť

pwc.com

© 2022 PricewaterhouseCoopers Slovensko, s.r.o. Všetky práva vyhradené. Názov "PwC" v tomto dokumente označuje spoločnosť PricewaterhouseCoopers Slovensko, s.r.o., ktorá je členom siete firiem PricewaterhouseCoopers International Limited, z ktorých každá je samostatným a nezávislým právnym subjektom.