



Principy důvěryhodnosti v cloudovém řešení Microsoft

Zdeněk Jiříček

Externí konzultant pro Microsoft ČR

Agenda

- Kybernetická bezpečnost
- Proč cloud
- Principy důvěryhodnosti
- Sjednocená identita (*Federated Identity*)

The Different Future is Today



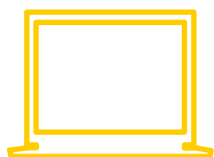
Microsoft: 7 principů vstříc globálním výzvám vůči kybernetické bezpečnosti



Požadavky uživatelů se vyvíjejí...

Moje PC

- ▶ Práce na cestách
- ▶ Bring Your Own PC



Moje zařízení

- ▶ Smartphony
- ▶ Tablety



Moje aplikace

- ▶ Cloud a hosting
- ▶ Sociální sítě



„Chtěl bych pracovat tak, jak mi to vyhovuje!“



Cloud mění přístup vedení k IT

Rychlost

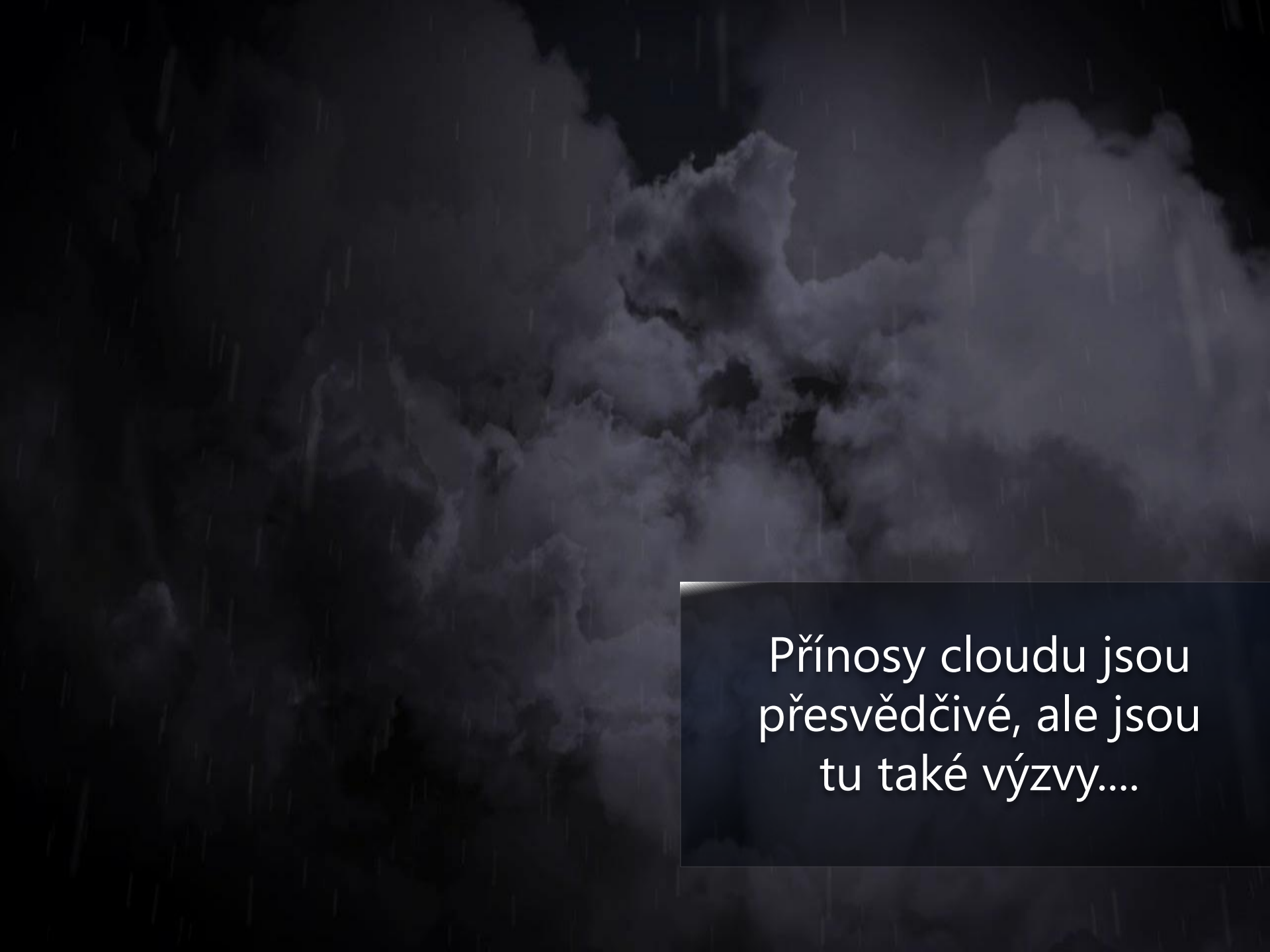
Náklady

Inovace

*Snížení nutnosti
počátečních investic*

*Nová očekávání pro
rychlost nasazení*

*Odstraňování bariér –
přístup k novým aplikacím
a službám*



Přínosy cloudu jsou
přesvědčivé, ale jsou
tu také výzvy....

Důvěryhodnost v cloudové řešení

Všichni se ptají - "Mohu důvěřovat cloudu?"

Hlavní obavy

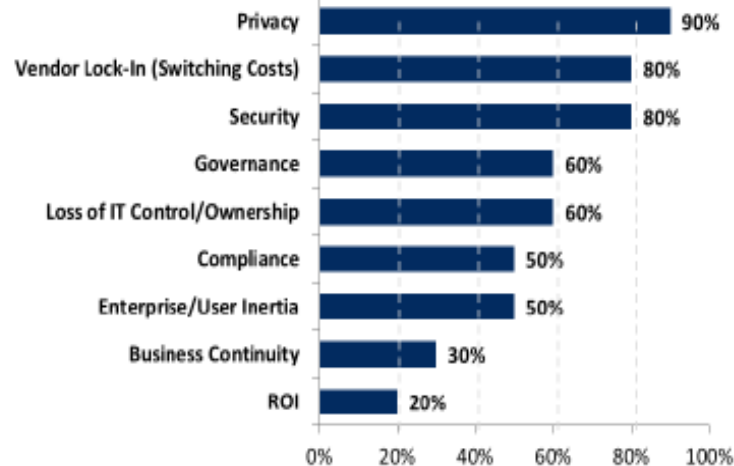
✓ Soukromí dat

✓ Ztráta kontroly

✓ Bezpečnost

✓ Soulad s předpisy

FIG. 19: PUBLIC CLOUD CONCERNS IN THE EUROPEAN PUBLIC SECTOR



Source: World Economic Forum 2009 Cloud Computing Survey.

Principy důvěryhodnosti

Soukromí
dat

*Respektujeme
soukromí vašich
dat*

Vedoucí pozice v
Transparentnosti

*Víte kde jsou
uložena vaše data,
kdo k nim má
přístup, a co s nimi
děláme*

Nezávislá
Verifikace

*Soulad
s průmyslovými
standards,
a verifikace třetími
stranami*

Bezpečnost
bez kompromisů

*Využití nejlepších
bezpečnostních
praktik*

Microsoft uvádí nový

Trust Center

Trust Centers

Office 365 Trust Center (CZ)

<http://www.microsoft.com/cs-cz/office365/trust-center.aspx>

Microsoft Office 365 BEZPLATNÁ ZKUSEBNÍ VERZE Česká republika (čeština) | Všechny weby společnosti Microsoft | Přihlásit

Prohledat tento web bing

Domů Co jsou to služby Office 365 Plány a ceny Technická podpora

Co jsou služby Office 365 / Důvěryhodnost a zabezpečení

Centrum zabezpečení služeb Office 365

Jakožto zákazník využívající služby Office 365 důvěřujete společnosti Microsoft, že bude schopna ochránit vaše data. Společnost Microsoft si této vaší důvěry velice váží a zároveň se usilovně snaží zajistit ochranu a bezpečnost vašich dat. Tímto způsobem se společnost Microsoft snaží držet si vedoucí pozici v oboru z hlediska využívání osvědčených postupů pro zajištění ochrany údajů, zabezpečení a dodržování předpisů.

Principy důvěryhodnosti v rámci služeb Office 365			
Je pro nás důležité zajistit ochranu vašich osobních údajů.	Vedoucí pozice v oblasti transparentnosti	Nezávisle ověřeno	Stálé zabezpečení
Naši snahou je chránit vaše osobní údaje.	Víte, kde jsou data uložena, kdo k nim má přístup a co s nimi provádíme.	Soulad se standardy World Class Industry ověřenými třetími stranami	Vynikající výsledky z hlediska zajišťování nejvhodnějších bezpečnostních postupů

Abychom dokázali získat vaši důvěru, již jsme aktivně odpověděli na celou řadu dotazů týkajících se zabezpečení a ochrany osobních údajů, na které by se podle organizace (pouze angličtina) Cloud Security Alliance měli všichni zákazníci ptát svého poskytovatele cloudových služeb. Produkty pokryté Centrem zabezpečení jsou uvedeny zde [zde](#).

Je pro nás důležité zajistit ochranu vašich osobních údajů.

Naši snahou je chránit vaše osobní údaje.

Podrobnosti

- **Žádná reklama:** Služby Office 365 nenabízí reklamní produkty na základě údajů o zákaznících. Neprohledáváme e-maily ani dokumenty zákazníků, abychom získali analytické informace, získávali data ani abychom je využívali pro reklamu či ke zlepšování služeb.
- **Žádné směšování dat:** V rámci služeb Office 365 budou vždy vaše data uchováвана mimo služby zákazníků.
- **Přenositelnost dat:** Zákaznická data v rámci služeb Office 365 patří zákazníkům. Zákazníci mohou svá data kdykoli podle svého vlastního uvážení odebrat. Další informace o

Windows Azure Trust Center

<http://www.windowsazure.com/en-us/support/trust-center/>

Windows Azure HOME PRICING DEVELOP COMMUNITY SUPPORT ACCOUNT

contact forums service dashboard faq sla legal trust center

Free trial

TRUST CENTER HOME

Security
Privacy
Compliance
Trust FAQ

Windows Azure Trust Center

Last Updated: March 2012

As a Windows Azure customer, you have entrusted Microsoft to help protect your data. Microsoft values this trust, and the privacy and security of your data is one of our top concerns. Microsoft strives to take a leadership role when it comes to security, privacy, and compliance practices.

Dynamics CRM Trust Center

<http://crm.dynamics.com/cs-cz/trust-center>

Microsoft Dynamics CRM | ČESKÁ REPUBLIKA

NASAZENÍ ŘEŠENÍ OBORY ZÁKAZNÍCI PARTNERSKÝ PROGRAM PODPORA KOMUNITA MARKETPLACE

Domů > Microsoft Dynamics CRM Online Centrum zabezpečení

Microsoft Dynamics CRM Online Centrum zabezpečení Trust Center

Jako zákazník produktu Microsoft Dynamics CRM Online důvěřujete společnosti Microsoft, že vám pomůže ochránit data. Společnost Microsoft si váží vaší důvěry a maximálně se snaží zachovat soukromí a bezpečnost vašich dat. Cílem společnosti Microsoft je získat vedoucí roli v ochraně a zabezpečení osobních údajů a dodržování průmyslových standardů, které se řídí následujícími principy.

Zkušební verze zdarma

Řešení můžete používat ve zkušební verzi až 30 dnů.

[VYZKOUŠTE SI CO NEJEDNĚ](#)

Soukromí dat v MS Online Services

Strategie rigorózních procesů a politik v oblasti soukromí dat

Žádné reklamy

- Žádné výstupy ze zákaznických dat pro reklamní účely
- Žádné skenování emailů a dokumentů za účelem analytických rozborů

Přenositelnost dat

- Zákaznická data v Office 365 jsou vlastnictvím zákazníka
- Zákazníci mohou kdykoliv svá data vyexportovat, až 90 dní po ukončení smlouvy

Žádné směšování datových prostorů

- Volba uchovávat zákaznická data v Office 365 odděleně od služeb pro spotřebitele (Windows Live, Hotmail, etc.)

Podrobnosti naleznete v [Microsoft Online Services Privacy Statement](#)

Transparentnost

Kde jsou uložena moje data?

- Microsoft poskytuje mapy uložení dat a jejich zeměpisné hranice
- Fyzická / doručovací adresa zákazníka určuje výběr datového centra
- Data jsou šifrována v tranzitu (SSL/TLS); úložiště – rozhodnutí zákazníka (AD RMS)

Kdo má přístup a k čemu?

- „Core Customer Data“ (těla zpráv a dokumentů) – přístup pouze ve výjimečných případech (prevence malware a řešení problémů), a je omezen na klíčový personál
- Trust Center vysvětluje mezní případy přístupu k datům v případě řešení problémů

Notifikace?

- Microsoft informuje zákazníky o změnách ve výběru datových center (data a služby)

„EU Model Clauses“ a další...

Microsoft je první a zatím jediný poskytovatel cloudové produktivity, nabízející:

Safe Harbor and EU Model Clauses

- Při zpracování osobních dat v cloudu lze vyhovět EU Directive 95/46/EC a zák. 101/2000 Sb.:
 - 1) Uzavřením smlouvy mezi Správcem a Zpracovatelem dat (Data Processing Agreement);
 - 2) Certifikací EU Safe Harbor vč. Onward Transfer Principle,
 - 3) Zahrnutím vzorové formulace „EU Model Clauses“ tj. „Standardní smluvní doložky“
- EU Model Clauses: zavazují Zpracovatele 1) řídit se pokyny Správce dat, a 2) chránit zákaznická data v souladu s EU legislativou

Data Processing Agreement (DPA)

- Je vyhověním požadavku na písemnou smlouvu mezi Správcem a Zpracovatelem dat (viz nahoře)
- Stanoví práva, povinnosti, a zodpovědnost při využití subkontraktorů; Eliminuje předávání osobních údajů třetím stranám; na přání zákazníka může obsahovat EU Model Clauses
- Microsoft DPA ve dvou formách: 1) se zákazníky Enterprise Agreement, a 2) jako příloha Microsoft Online Subscription Agreement (MOSA)

Proč nezávislá verifikace?

“Potřebuji jistotu, že Microsoft postupuje správně”

Podpora a přijetí **průmyslových standardů** zajišťuje nasazení postupů a řídicích metod za účelem ochrany zákaznických dat

MS neumožňuje audit datacenter zákazníky, ale využívá **nezávislé verifikace** řízení bezpečnosti, soukromí, a kontinuity provozu

Transparentnost



Toto šetří čas a peníze pro všechny, a umožňuje Microsoft Online Services poskytovat ujištění kvality všem zákazníkům

Microsoft Online Services Verifikace

První a zatím jediný poskytovatel cloudové produktivity, nabízející ISO27001, ISAE3402, EU Model Clauses, FISMA, a HIPAA



ISO27001

- ISO27001 je jedním z nejlepších měřítek bezpečnosti (důvěrnost, integrita, dostupnost služeb)
- Office 365 je první službou cloudové produktivity, která implementovala přísná ISO bezpečnostní pravidla na fyzické, logické, a procesní úrovni řízení (Azure Information Security Mgmt System - ISMS)

SAS 70, nyní SSAE 16, a ISAE 3402

- SAS 70 reporty poskytovaly zákazníkům náhled do procesů poskytovatelů služeb (zejména v USA). Od 15/6/11 nahrazeno SSAE 16 a ISAE 3402.
- Office 365 má jak SSAE 16, tak ISAE 3402 certifikace pro uznání v USA, v Evropě, i jinde ve světě
- International Standard on Assurance Engagements (ISAE) 3402 – atest kvality a efektivnosti řízení u poskytovatelů služeb, k dispozici pro své zákazníky a jejich auditory

Poslední stav souladu s předpisy

Klíčové standardy

Certifikace	Cílová skupina	Microsoft Online Services
ISO 27001	Všichni zákazníci	Nyní k dispozici
EU Safe Harbor	EU zákazníci	Nyní k dispozici
SSAE 16 (Statement on standards for Attestation Engagement) Type I compliance	US zákazníci	Nyní k dispozici
ISAE 3402 International standards for Attestation Engagement	Všichni zákazníci	Nyní k dispozici
SSAE 16/ISAE 3402 Type II compliance	Všichni zákazníci	Nyní k dispozici (od 20/6/12)
FISMA	US Government	Nyní k dispozici (od 3/5/12)
HIPAA	US zákazníci	Nyní k dispozici
EU Model Clauses	Všichni zákazníci	Nyní k dispozici
Data Processing Agreement	Všichni zákazníci	Nyní k dispozici

Politika informační bezpečnosti (cloud)

Založena na ISO 27001/27002 (C-I-A Confidentiality, Integrity, Availability),
definuje Standardní provozní procedury (Standard Operating Procedures)

1. Bezpečnostní politika
2. Organizace informační bezpečnosti
3. Správa prostředků (Asset Management)
4. Bezpečnost v oblasti lidských zdrojů
5. Bezpečnost fyzická a vliv na životní prostředí
6. Správa provozu a komunikací
7. Řízení přístupu
8. Pořizování IS, jejich vývoj a údržba
9. Řízení incidentů v informační bezpečnosti
10. Zajištění kontinuity provozu (Business Continuity Mgmt)
11. Soulad s legislativou

Architektura cloudu Microsoft Global Foundation Services

Cloudové služby

Consumer
Services

Enterprise
Services

Zákaznické
aplikace

Microsoft
Office 365



Microsoft
Dynamics CRM Online



Windows Intune

Platformové služby



Windows Azure™

Cloudová infrastruktura



Infrastructure



Security



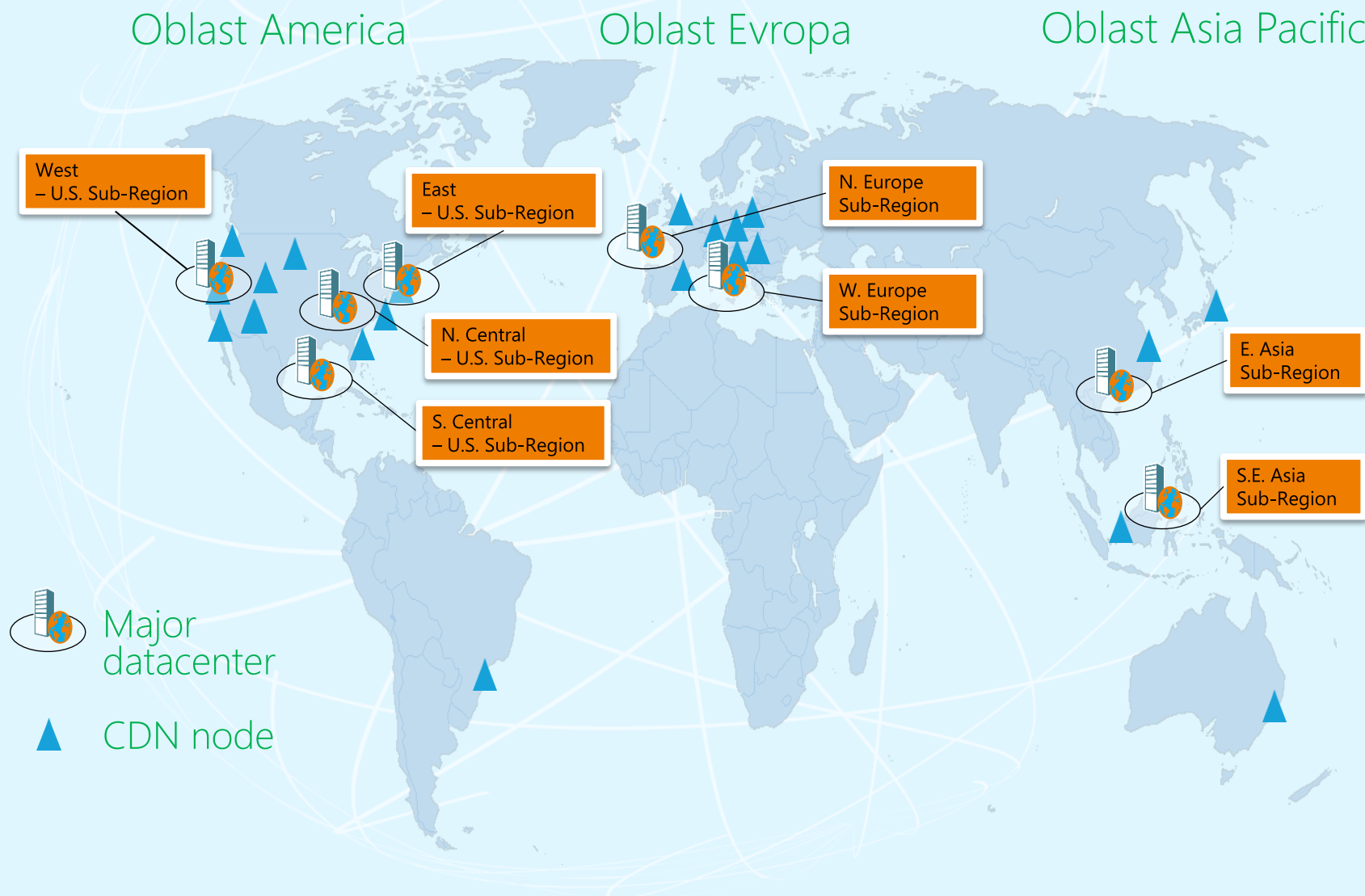
Global Delivery



Sustainability

Global Foundation Services

Windows Azure – Globální přítomnost



Vrstvy zabezpečení

Uživatel

- Správa účtů, osvěta a školení, aktivní ochrana
- Access Control Service – otevřený, interoperabilní

Data

- Šifrování při uložení umožněno (záleží na zákazníkovi)
- Podpora SSL pro všechny datové přenosy

Aplikace

- Volba běhu aplikací v nižší úrovni důvěry
- Uživatelské účty s nižšími systémovými právy

Host Server

- Omezená / zajištěná (hardened) verze Windows Serveru
- Hypervisor stanovuje bezpečnostní perimetr nezávisle na OS

Síť

- Série firewallů omezující přístup k virtuálním strojům
- VLANs a filtrování paketů

Fyzická

- Silná fyzická ochrana Global Foundation Services
- ISO 27001, SSAE 16, FISMA, a další

Vrstva

Obrany

Měřítko bezpečnosti prostřednictvím STAR

<https://cloudsecurityalliance.org/>

**STAR – Security, Trust & Assurance
Registry**

**Standard vytvořený
Cloud Security Alliance (CSA)**

Cloud Security Alliance „**Cloud Controls Matrix (CCM)**“ popisuje základní principy bezpečnosti jako vodítko pro cloudové firmy i pro potenciální zákazníky v celkovém hodnocení bezpečnostních rizik.



Office 365 Security Response in the Context of the CSA Cloud Control Matrix Controls CO-01 through CO-03

Control ID in CCM	Description (CCM Version 6.1.1, Final)	Microsoft Response
CO-01 Compliance - Audit Planning	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	Our goals are to operate our services as securely as possible and to give you accurate assurances about our security. We have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Each year, we undergo third-party audits by internationally recognized auditors to validate that we have independent attestation of compliance with our policies and procedures for security, privacy, continuity and compliance. Audit reports are available under NDA upon request. Monitor and review the Information Security Management System (ISMS) is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.3, for more information review of the publicly available ISO standards we are certified against is suggested.
CO-02 Compliance - Independent Audits	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e. internal/external audits, certifications, vulnerability and penetration testing).	For more information see CO-01 or the Trust Center for our current certifications and third party attestations.
CO-03 Compliance - Third Party Audits	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	Microsoft Online Services contractually requires third parties to maintain equivalency with Microsoft Online Services Information Security Policy. In addition, Microsoft Online Services requires that third parties undergo an annual third party audit or arrange to be included in Microsoft Online Services annual third party audit. Addressing security in third party agreements and third party service delivery management is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2, 8.0, 10.2, for more information a review of the publicly available ISO standards we are certified against is suggested.

Microsoft

Online Services Standard FY11 Response on Security | Page 7

Microsoft Office 365 a Windows Azure Standard Response on STAR

Podrobnosti bezpečnosti a soukromí v Office 365 jsou mapovány na Cloud Control Matrix (CCM) a ISO certifikaci

Identity Management (IdM) v cloudových službách

Cloud a hybridní prostředí přinášejí nové výzvy pro IdM

Řízení přístupu

Řízení přístupu
pomocí IP protokolu,
federace, a možnost
vícefaktorové
autentizace

Single Sign-On

Zajištění
Single-Sign-On
pro lokální
i cloudové aplikace

Directory Management

Centralizovaná správa
objektů pro lokální
i cloudové služby

Nativní IdM v Office 365

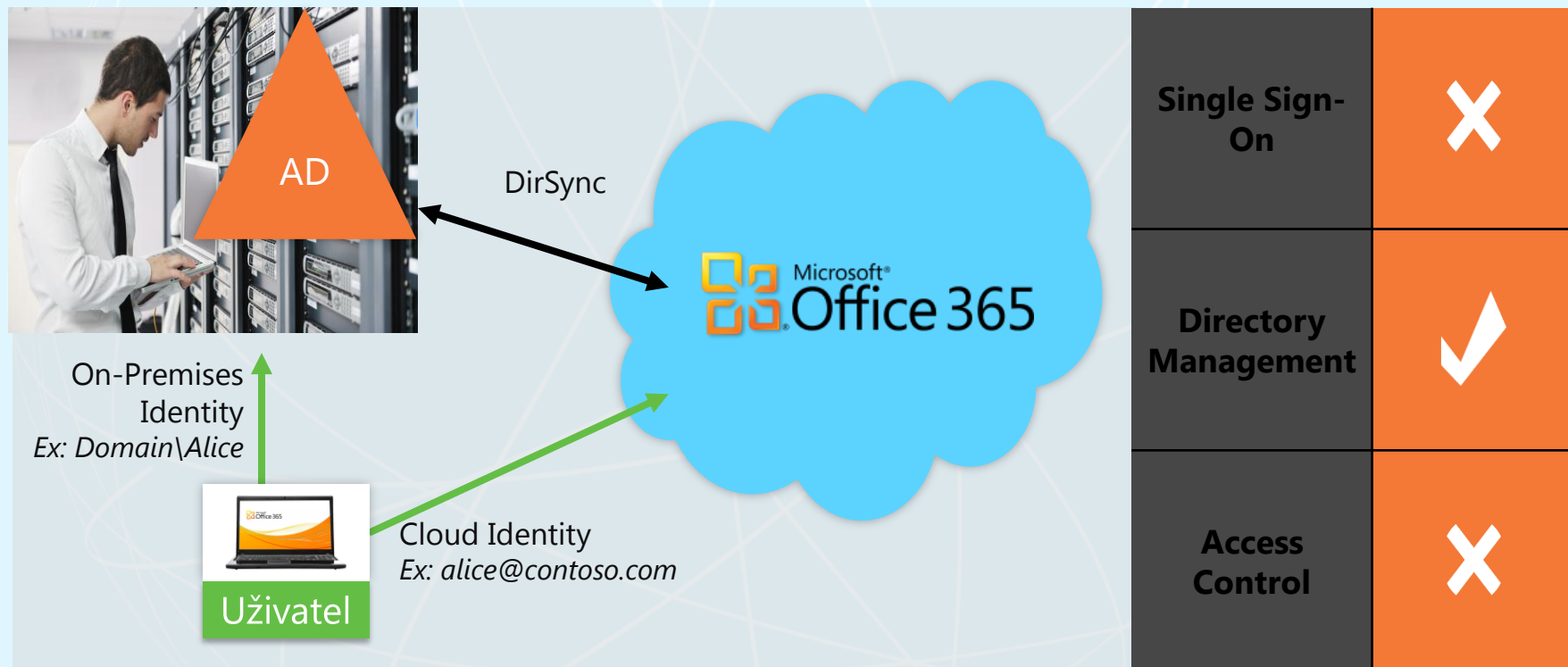
- Nezávislá správa identit v Office 365
- Bez nároků na lokální infrastrukturu
- Důsledek: separátní správa uživatelských účtů lokálně a v cloudu



Vhodné pro malé úřady bez místní síťové správy

Office 365 IdM s místním AD

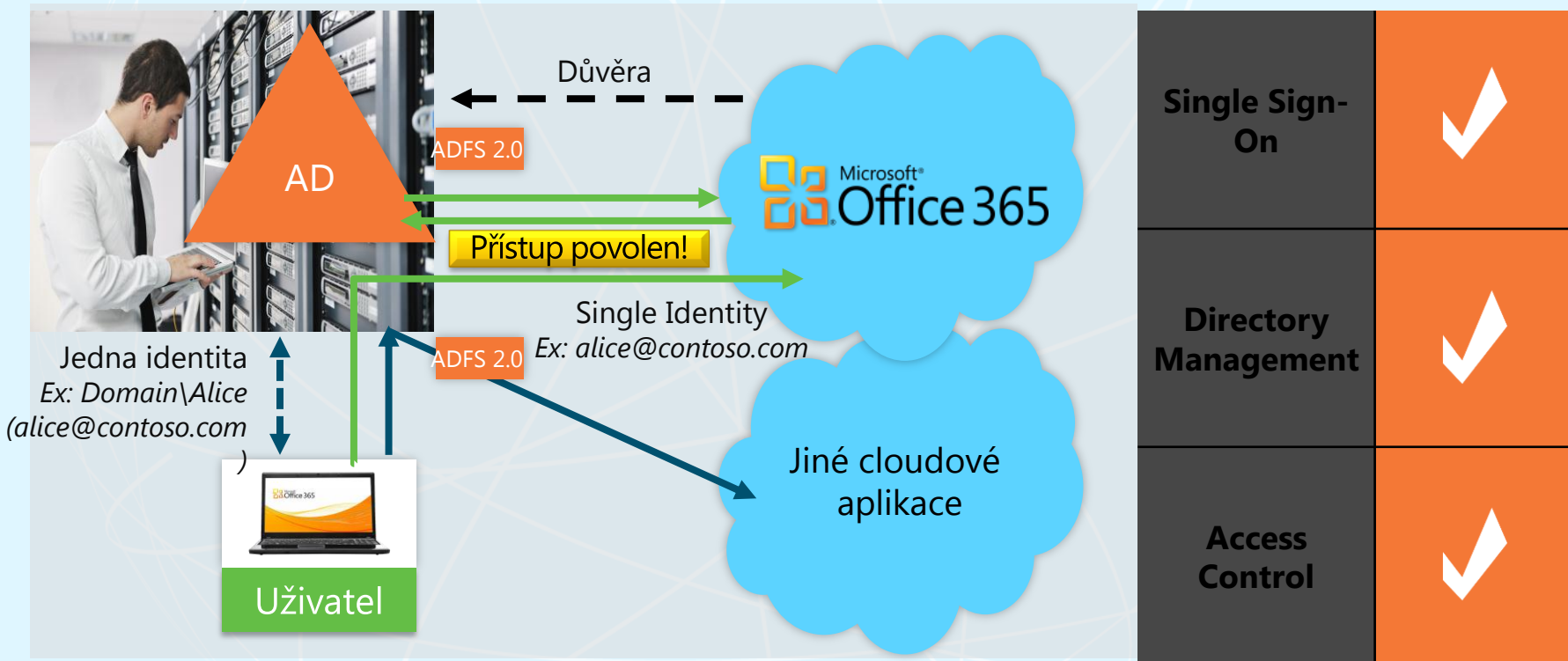
- Nezávislá správa identit v Office 365
- DirSync zajišťuje synchronizaci Active Directory s Office 365
- Výsledek: pravidelná synchronizace lokálních účtů s cloudem



Vhodné pro střední velikost úřadů s místní IT správou (Active Directory), ale s omezenými požadavky na IdM

Federace Office 365 s lokálním IdM

- Sjednocená identita pro lokální a cloudové služby Office 365
- Dynamický Single Sign-on pro lokální a cloudové služby Office 365
- Stejný princip federace lze využít i pro další cloudové služby



Vhodné pro velké úřady s místní IT správou (Active Directory), a s požadavkem Single Sign-On

Výhody federace s místním adresářem

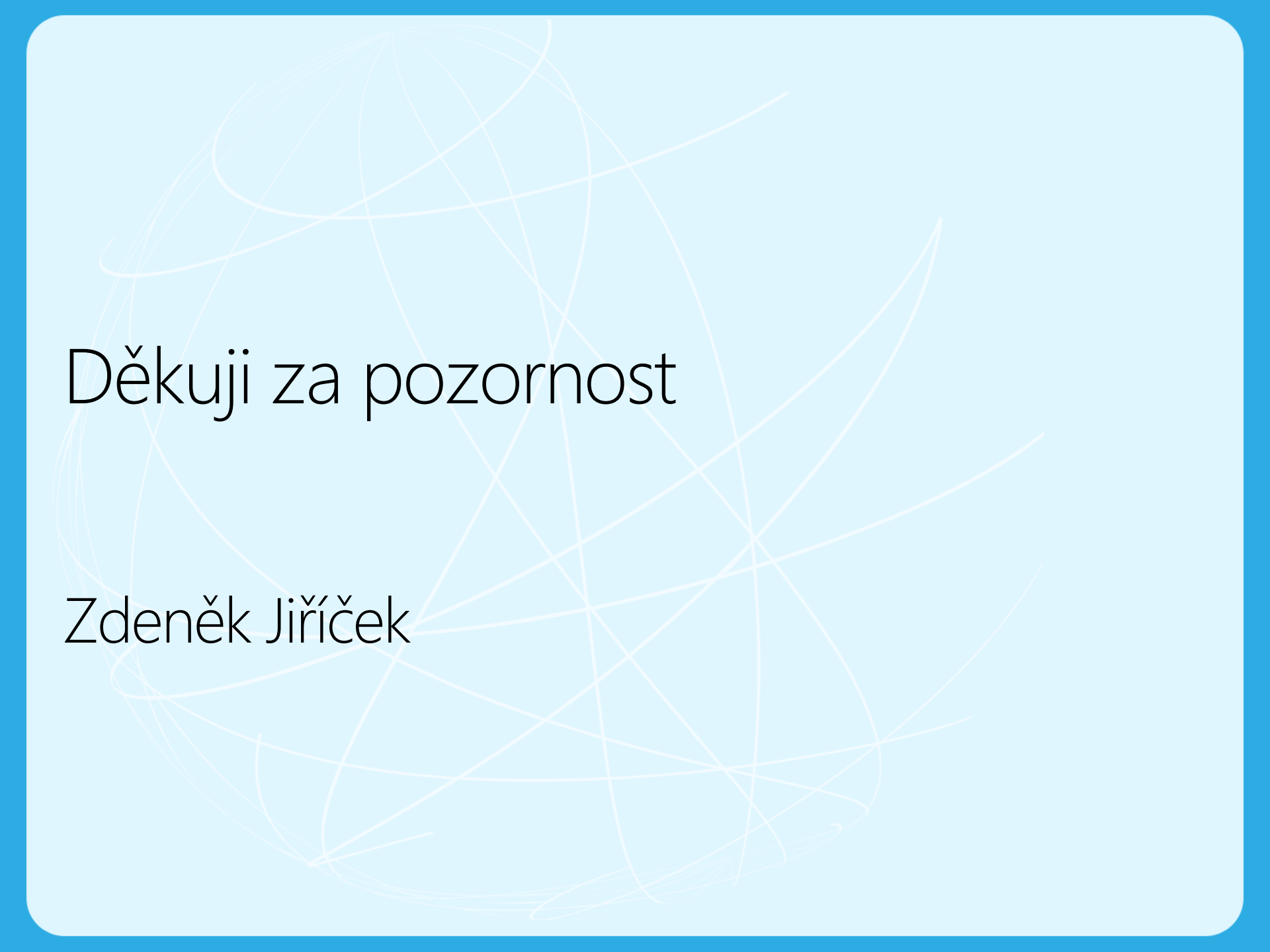
- Jedno místo pro síťovou správu
 - Uživatelé, skupiny, zabezpečené skupiny
 - Hesla a jejich pravidla „necestují“ mimo organizaci
 - Spravuje také síťové prostředky i aplikace
- Podpora dynamického Single-Sign-On
- Podpora vícefaktorové autentizace (OTP, Token, Smart card)
- Centrální správa přístupových práv (autorizace)
- Podpora hybridních scénářů (lokální + cloud)
 - (např. integrace Exchange Online)

Shrnutí

- Cloud zvyšuje obavy o soukromí dat, bezpečnost a transparentnost procesů, soulad s právem
- Centrum zabezpečení Microsoft
- Význam ISO 27001, ISAE 3402
- EU Data Protection Directive, zák. 101/2000 Sb.
 - Smlouva o zpracování dat, EU Safe Harbor, EU Model Clauses
- Asociace Cloud Security Alliance
 - Cloud Controls Matrix – jednotné srovnání dodavatelů
- Federace identit: vyšší bezpečnost a nižší náklady

Reference

- Office 365 / Azure Trust Centers
 - <http://www.microsoft.com/cs-cz/office365/trust-center.aspx> (Česky)
 - <http://www.windowsazure.com/en-us/support/trust-center/>
- Microsoft Online Services Agreement (MOSA)
 - vč. dodatku „Smlouvy o zpracování dat“ – spotřebitelská verze
 - <https://mocp.microsoftonline.com/Site/MOSA/MOSA-en-EMEA.htm?containerId=FullAgreement>
- Microsoft Online Services Privacy Statement
 - <http://www.microsoft.com/online/legal/?langid=en-us&docid=7>
- Cloud Security Alliance (CSA)
 - <https://cloudsecurityalliance.org>
 - Odtud CSA Security, Trust & Assurance Registry (STAR)
 - <https://cloudsecurityalliance.org/star/>
- Rozhodnutí Evropské komise 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.



Děkuji za pozornost

Zdeněk Jiříček