VIAVIS střežíme podstatné

Informační systémy a bezpečnost

Kybernetická a informační bezpečnost I

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Cíl přednášky

- **Bezpečnostní pohled na informační systémy**
  - Liší se od funkčního – leckdy podstatně, ***proč?***
  - Informační systém je subjektem ochrany

Proč informační systémy

- Cílem útoků:
  - Informace (reprezentována daty)
  - Informační systém (v celém kontextu)
  - Lidé informační systém využívající
  - Sociální systémy (stát, komunita…)

- Dopady útoků – mohou být extrémní:
  - Politická rozhodnutí
  - Likvidace firem
  - Likvidace osob

Různé pohledy na informační systémy

- Informační systém x ICT systém
- Možné pohledy na ICT systém
- Mikro IT x makro IT
- Architektura, vrstvy, provoz

Informační systém

- Informační systém – systém, který:
  - Sbírá informace
  - Transformuje informace na data
  - Zajišťuje přenos, zpracování a uchování dat
  - Data prezentuje a interpretuje
  - Zajišťuje archivaci nebo ničení dat

- Je informační systém vždy ICT (počítačový) systém?
  - Kartotéka u lékaře
  - Pořadač vizitek

Informační systém x ICT systém

- ICT systém - informační a komunikační systém využívající IT techniku

- Komunikační a informační systémy splývají
- Komunikační systémy jsou samy informačními systémy

- **ICT systém je pouze podmnožinou informačního systému**
- Je chybou zužovat bezpečnostní aspekty pouze na ICT systém

Pohledy na IS

- Manažerský pohled, Business pohled
- Black Box x Crystal Box
- Mikro ICT systémy x makro ICT systémy
- Funkční pohled
- Procesní pohled
- Architektonický pohled
- Pohled dle rolí

- **Bezpečnostní přístup – musí zahrnovat všechny pohledy a aspekty**

Business pohled – klíčové otázky

- **Do jaké míry IS ovlivňuje chod organizace?**
- **Jak je organizace na IS závislá?**
- **Existují alternativy?**
- **Jaká je hodnota IS?**
  - Odpovědi dává analýza rizik

Manažerský pohled – silný vliv na bezpečnost

- Rozhodnutí k neznalosti:
  - *„Jsem přetížen, zahlcen, nechci tomu rozumět“*
  - *„Od toho mám ajťáky“*
- Iluze znalosti:
  - *Čtenář časopisů a účastník konferencí*
  - *Znalost detailu bez nadhledu*
  - *Znalost minulosti*
  - *Mikromanagement*

Manažerský pohled – silný vliv na bezpečnost

- Manažerský nadhled a manažerská pokora:
  - Přehled základních principů a jejich pochopení
  - Umění naslouchat a hodnotit
  - Schopnost dělat správné závěry a rozhodnutí
  - Schopnost nést odpovědnost
- Proč manažerský pohled:
  - Manažer rozhoduje, manažer bezpečnosti přesvědčuje a argumentuje
  - Srozumitelný jazyk
  - Využití sociotechnik – manažer bezpečnosti musí mít povědomí o psychologii

Manažerský pohled požadavků

- Manažerský problém:
  - Jak se orientovat, kde získat relevantní informace a nadhled?
  - Manažeři jsou přehlceni informacemi/šumem
  - Problém nutnosti rychlých rozhodnutí/žádné podklady
- Experti mluví nesrozumitelným jazykem
- Bez elementárních znalostí nelze vypěstovat manažerský cit
- **PROČ - manažerský pohled je zdrojem vážných incidentů**

Manažerská „selhání“ díky neznalosti

Sdílet článek

Útok na ŘSD nabývá rozsáhlých rozměrů: Úřad zvažuje, zda hackerům za data zaplatit

Ekonomika
10. 6. 2022 11:06

Ředitelství silnic a dálnic zvažuje, zda má zaplatit výkupné ve výši desítek milionů korun, které po něm požadují hackeři. Státní organizace se v květnu stala terčem kybernetického útoku a přišla o celé účetnictví a všechny smlouvy uložené na discích. Hackeři výměnou za peníze nabízejí, že ŘSD odblokují přístup do jeho systémů a úložišť.

reklama

https://zpravy.aktualne.cz/ekonomika/doprava/rsd/r~c124bcbee89011ec9ae20cc47ab5f122/

Manažerská „selhání“ díky neznalosti

Systém veřejné správy napadli hackeři, útok se týkal Prahy i ministerstva práce

AKTUALIZOVÁNO 5. 3. 2021

Systém veřejné správy napadli ve čtvrtek hackeři. O masivním kybernetickém útoku informoval na Twitteru pražský primátor Zdeněk Hřib (Piráti), data magistrátu podle něj nebyla poškozena. Jedním z cílů

https://ct24.ceskatelevize.cz/domaci/3278730-system-verejne-spravy-napadli-hackeri-utok-se-tykal-prahy-i-mpsv?fbclid=IwAR2KTRD0o4re2rGio-hpIqQmROzmk_NVMVaV47pCdDK_D-3wZQ-k7AmBcqA

VIAVIS

Manažerská komunikace – co nefunguje

6 000 českých firem bude muset řešit kybernetické zabezpečení

Je bláhové si myslet, že hackerské útoky se soustřeďují pouze na úřady či nemocnice. Ve stejném ohrožení jsou i soukromé firmy. Zde je problém o to větší, že většinou nejsou na podobné útoky připraveny a dosud je vůbec neřeší.

Bezpečné, dvoufaktorové přihlášení do důležitých systémů, zavedení odolné kryptografie, zálohování dat či řízení rizik je pro ně zcela neznámá oblast.

Přitom útoky na ně mohou způsobit daleko větší škody, než útoky na běžné úřady. Hackeři dnes dokážou na dálku ovládnout dávkovače chemických látek či výrobní linky potravinářských firem.

Směrnice NIS 2 bude povinná a bude se týkat jen v ČR tisíců nových subjektů. Přitom maximální pokuta za její nedodržení bude 10 000 000 Kč, nebo 2 % z celkového celosvětového ročního obratu společnosti.

https://proid.cz/smernice-nis-2-koho-se-tyka-a-jak-ji-aplikovat-v-praxi/

IS typu Black Box

- Black box – interní architektura systému se nezkoumá, pouze jsou definovány:
  - Vstupy
  - Transformace - funkce, vlastnosti (neřeší se jak)
  - Výstupy
- Typický pohled uživatele, managera
- Prvky systému typu black box – např. komerční software
- Co dělá excel?
- **Praxe víry – existuje cesta limitace rizik?**

IS typu Black Box

- Black box - diskuse:
  - WIN, Mac OS, iOS, Android – jaká je jejich míra bezpečnosti?
  - Bezpečnostní aspekty black box, výhody, nevýhody
  - Kdy je možné z bezpečnostního hlediska využít black box?
  - Čím je dána bezpečnost systému black box
  - Jak lze ošetřit bezpečnostní aspekty systému black box
  - Kyber bezpečnost x právní instrumenty – smlouvy, odpovědnost

IS typu Crystal Box

- Crystal Box – je známa podrobná architektura a všechny prvky systému:
  - Vstupy
  - Transformace - funkce, vlastnosti:
  - Prvky systému, jejich vlastnosti, funkce
  - Vazby mezi nimi – funkční, bezpečnostní
  - Interní architektura
  - Výstupy
- Pohled architekta, designéra, správce, auditora
- Pohled manažera – opět důvěra k profesionálovi
- Prvky systému – např. Open Source software

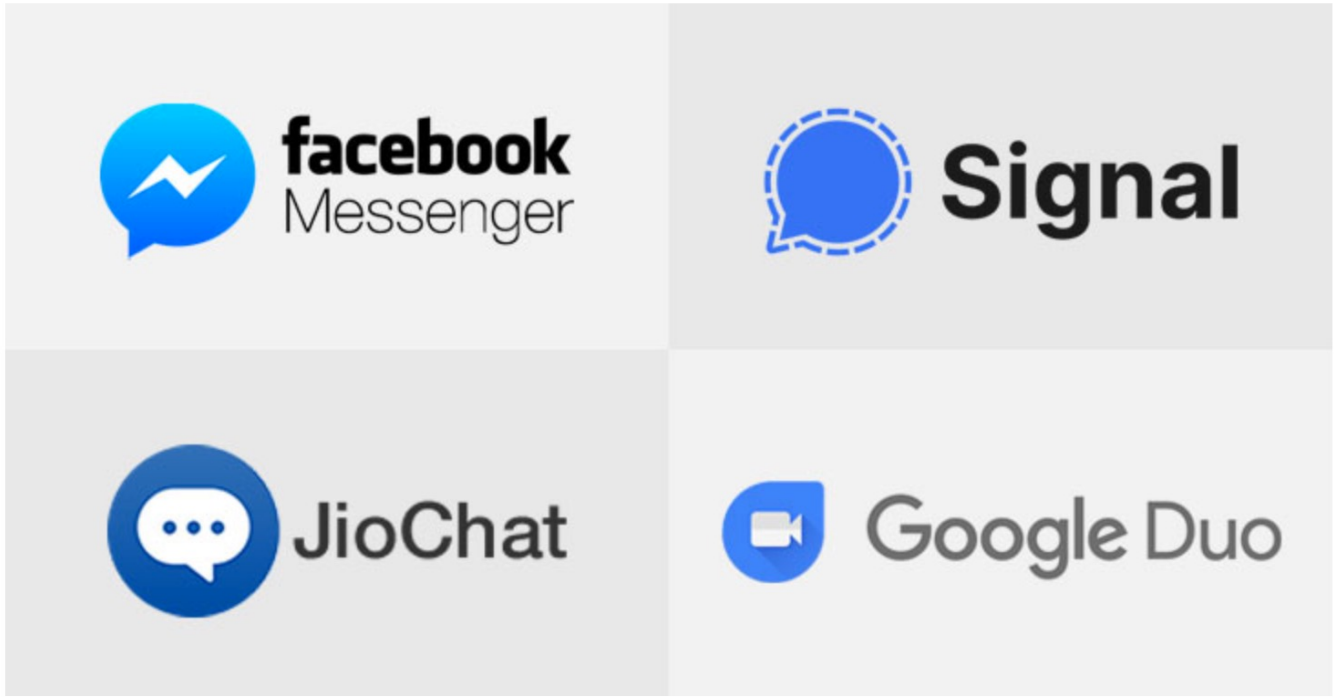
IS typu Crystal Box

- **Diskuse o Crystal Box:**
  - Bezpečnostní aspekty, výhody, nevýhody
  - Čím je dána míra bezpečnosti?
  - Kdy je výhodné použít crystal box x black box
  - Kritické místo?
  - Právní aspekty
  - Vynutitelnost odpovědnosti za open source SW

Svět víry – vznik Zero Day Vulnerabilities

Google Details Patched Bugs in Signal, FB Messenger,

January 20, 2021 Ravie Lakshmanan



https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

VIAVIS

Odezvy výrobců

- Signal (fixed in September 2019) - A audio call flaw in Signal's Android app made it possible for the caller to hear the callee's surroundings due to the fact that the app didn't check if the device receiving the connect message from the callee was the caller device.

https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

- JioChat (fixed in July 2020) and Mocha (fixed in August 2020) - Adding candidates to the offers created by Reliance JioChat and Viettel's Mocha Android apps that allowed a caller to force the target device to send audio (and video) without a user's consent. The flaws stemmed from the fact that the peer-to-peer connection had been set up even before the callee answered the call, thus increasing the "remote attack surface of WebRTC."

- Facebook Messenger (fixed in November 2020) - A vulnerability that could have granted an attacker who is logged into the app to simultaneously initiate a call and send a specially crafted message to a target who is signed in to both the app as well as another Messenger client such as the web browser, and begin receiving audio from the callee device.

- Google Duo (fixed in December 2020) - A race condition between disabling the video and setting up the connection that, in some situations, could cause the callee to leak video packets from unanswered calls.

Mikro informační systémy

- Mikro ICT systémy:
  - Zjednodušeně – lze definovat jejich perimetr
  - Interní ICT systémy korporací, firem, organizací veřejné správy, domácností
  - Feudální charakter řízení – vlastníkem
  - Větší možnosti vynucení bezpečnostní politiky
- Častý cíl interních útoků
- Rychlá reakce na incident
- Omezené zdroje (opravdu?)

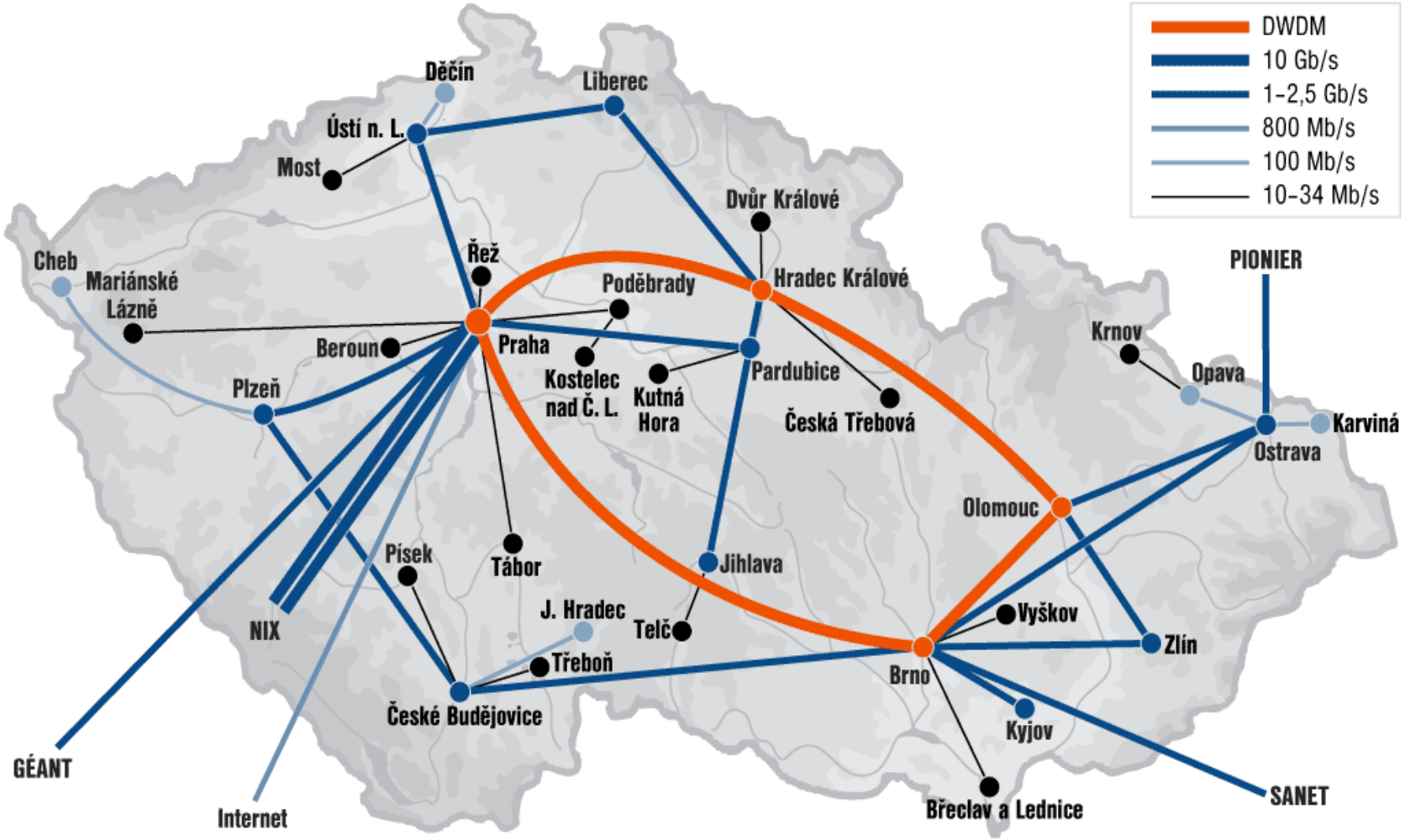
- **Výhody?**

Makro informační systémy

- Makro systémy:
  - Systémy na úrovni velkých celků – státu, silových složek, nadnárodních organizací
  - Velmi obtížně lze definovat jejich perimetr
  - Jiná architektura a charakter, než mikro ICT systémy
  - Nelze obvykle uplatnit feudální (hierarchické) řízení
- Pomalejší reakce
- Problematická definice odpovědnosti
- Obtížná vynutitelnost pravidel hry
- Jakou mají vůbec strukturu? Je hierarchická – pouze u této lze velet…

- ***Diskuse: Jak lze „vypnout internet“?***

Jak lze vypnout internet?



VIAVIS

Makro systémy - internet

- Internet byl navržen s odolností vůči útokům zvenčí, **ne zevnitř**
- Návrh neobsahuje principy pro trasování uživatelů
- Nemá mechanismy rezistence proti nedůvěryhodným uživatelům
- **Pokrývá globální prostor – různé jurisdikce**
- Obrovská míra heterogenity
- Bezpečnost je na připojeném systému

VIAVIS

Informační systémy nad internetem - kyberprostor

- Hlavní výhody:
  - Nízká cena
  - Dostupnost připojení – rozšíření Internetu
- Problémy k řešení:
  - Řízení kapacity přenosu – QoS
  - Kapacita internetu se sdílí
  - Bezpečnost při sdílené komunikaci – přenos nepřátelským prostředím
  - Kdo komunikace sleduje?
  - Neznámá rizika a vlivy na bezpečnost

Informační systémy nad internetem

- Klientské systémy – bezpečnostní pohled
  - K informačnímu systému přistupuje klient:
  - Vlastní uživatel – lze vynutit pravidla hry
  - Cizí oprávněný uživatel – vynucení pravidel hry je obtížnější
  - Anonymní uživatel
  - Identita uživatele – autentizace, autorizace
  - Bezpečnost přistupujícího zařízení – různé bezpečnostní úrovně
  - Právní odpovědnost – bankovní systémy

Procesní pohled

- Informatika je chápána jako množina procesů, kterými je zajištěno zpracování informací
- Příklady informatických procesů:
  - Vstupy dat – automatizované, ruční
  - Správa infrastruktury
  - Správa uživatelských požadavků
  - Provoz informačních systémů
  - Rozvoj infrormačních systémů
  - Řízení ICT
  - Podpůrné procesy – nákup, ekonomika, kontrola
- Procesní pohled dnes v ICT světě převažuje
- Velice často ICT procesy neobsahují bezpečnostní aspekty – ona otřepaná hesla v obálkách

Příklad některých procesů

- Risk management – jak identifikovat a zvládat rizika
- Business continuity – jak co nejefektivněji zvládnou výpadek
  - Zálohovací schémata
  - Havarijní plány
  - Plány obnovy
- Incident management – jak efektivně identifikovat a zvládnou incident
- Identity management
  - Uživatelé a řízení jejich přístupových oprávnění
  - Procesy zavedení nového, změna, ukončení prac. Poměru
- Release management
- Change management

Procesní pohled na informatiku

- Trend – definice **katalogu služeb**
  - Definice služby, kvalitativní i kvatifikace
  - Požadavky na službu - SLA
  - Odpovědnost a role
  - Způsob poskytování služby
  - Bezpečnostní požadavky (důvěrnost, dostupnost integrita…)
  - Cena služby

Typy katalogu služeb

- **Business katalog služeb**
  - Definice služby pro management:
    - Elektronická pošta
    - Správa uživatelů
    - Provoz ERP
- ***Navrhněte:***
  - Odpovědnost a role
  - Způsob poskytování služby
  - Cena služby

Typy katalogu služeb

- **Technický katalog služeb**
  - Pod business katalogem služeb, je na něj navázán
  - Zohledňuje vazby mezi systémy
  - Spojuje technické služby
    - Server s virtuálem pro více služeb
    - Sdílení infrastruktury
    - Provoz ERP

- ***Navrhněte:***
  - Technický katalog pro elektronickou poštu

Bezpečnost IT rolí

- Role v ICT procesech:
  - ICT manager
  - ICT administrátor
  - Uživatelská podpora – helpdesk
  - Solution architekt
  - Project mnanager
  - Aplikační správce
  - Auditor
  - Zákazník ICT služeb
- Organizační struktura je optimalizována pro procesní řízení
  - Podceňované hrozby – socioútoky, útoky „na role“
  - ***Které role lze sdílet jednou osobou? Diskuse***

Bezpečnost IT rolí – personální bezpečnost

- Zaměstnanec v ICT či bezpečnostní roli
  - Vysoká míra rizika
  - Omezená možnost kontroly
  - Kreativita v obcházení pravidel
  - Zaměstnanec po výpovědi
  - Rodinní příslušníci

Bezpečnost IT rolí – personální bezpečnost

- Některé nástroje personální bezpečnosti (bude více v KB II)
  - Zbavení anonymity
  - Vědomí o hodnotách – přijetí zodpovědnosti
  - Školení a vzdělávání
- Definice pravidel hry:
  - Politiky a směrnice
  - Etické kodexy
  - Smlouvy a závazky mlčenlivosti
- Firemní kultura a prostředí
  - Sociotechniky
  - Důsledná kontrola – audity, pen testy

Bezpečnost IT rolí – personální bezpečnost

- Rizikové faktory:
  - Výpověď
  - Podcenění výpovědi ne manažerských pozic
  - Podcenění procesního a technického řešení
  - Trénink manažerů, jak se rozejít
  - Pocit křivdy – nespravedlnost, nedodržení podmínek, demotivace
- Vážná rodinná situace
- Charakter zaměstnance - chamtivost

IT systémy po vrstvách

- Infrastruktura
  - Vše, co je potřeba k provozu aplikací
- Aplikační vrstva
  - Aplikační software, ERP systémy…
- Vrstva služeb
  - Řízení, správa a vše okolo

Infrastruktura

- Fyzická vrstva:
  - Datové spoje
  - Hardware
- Software infrastruktury:
  - SW spojený s HW – ovladače, speciální komunikační software, protokoly
  - Operační systémy
  - Databázové systémy
  - Komunikační software
- Bezpečnostní software

Infrastruktura

- Bezpečnostní problémy:
  - Důvěrnost – autentizace, autorizace, nakládání s vadnými díly, otevřené přístupy, infrastrukturní software - zabezpečení
  - Dostupnost – business continuity – zálohování a obnova funkcí, odezvy, přístupy, servisní smlouvy
  - Integrita – nedochází ke změnám uložených dat? Jsou kompletní?
- Problém dneška – heterogenní prostředí, mobily, tablety…
- ***Kde je optimum mezi uživatelským komfortem a náklady na** bezpečnost?*

Infrastruktura

- Bezpečnostní problémy:
  - Black Box x Crystal Box
- Black Box:
  - Software (ale i hardware) obvykle na komerční bázi, není k dispozici úplná dokumentace, zdrojové kódy
  - Microsoft, Apple, Oracle, CheckPoint, McAfee, Symantec …
- Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit
- Crystal Box:
  - Většinou Open Source, je k dispozici zdrojový kód a dokumentace
  - Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit
- ***Publikace Back Doors – co je ještě důvěryhodné?***

Infrastruktura

- Bezpečnostní problémy:
  - Black Box x Crystal Box
- Black Box:
  - Software (ale i hardware) obvykle na komerční bázi, není k dispozici úplná dokumentace, zdrojové kódy
  - Microsoft, Apple, Oracle, CheckPoint, McAfee, Symantec …
- Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit
- Crystal Box:
  - Většinou Open Source, je k dispozici zdrojový kód a dokumentace
  - Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit
- ***Publikace Back Doors – co je ještě důvěryhodné?***

Aplikační vrstva

- Zjednodušeně – software, který pracuje nad infrastrukturou, využívá ji a zpracovává data – interpretuje na informace
- Členění je různé:
  - Podnikové systémy – ERP, CRM, APS, MES, Document Management, Workflow Management…
  - Kancelářské systémy – Office, mail…
- Bezpečnostní problémy:
    - Důvěrnost – přístupy, způsob uložení dat, přístupy podpory, logy
    - Dostupnost – SLA, business continuity
    - Integrita – jsou data korektní, zpracovávají se popsaným způsobem? Je aplikační logika dokumentována a testována?

Aplikační vrstva – bezpečnostní problémy

- Licenční čistota, podmínky rozšíření licencí
- Vendor Lock
- Podmínky podpory – SLA, obsah, podmínky, řešení incidentů
- Práce s datovými médii
- Know how – dostupnost implementačních konzultantů
- Vzdálené přístupy – neexistence NDA
- Stabilita dodavatele
- Struktura dat
- Aplikační logika
- Archivace dat
- Formát dat
- Odezva a rychlost

Cloud - specifikum

- Stará myšlenka nově marketingově uchopená
  - Jak mámit z uživatelů více peněz ☺
  - Obecně nelze cloud ani zatratit ani nekriticky doporučit
- Princip:
  - Sdílení zdrojů je levnější
  - Platím jen to, co opravdu potřebuji
- Obsah cloudu:
  - Uložiště dat
  - Synchronizace, sdílení dat
  - Poskytování aplikací
  - Zajištění provozu – SLA

Cloud - specifikum

- Bezpečnostní rizika:
  - Data nejsou pod kontrolou – i „triviální operace“ (výmaz dat…)
  - Jurisdikce, kde jsou data uložena
  - Bezpečnostní řetězec - kdo má k datům přístup – poskytovatel, telco služby
  - Důvěryhodnost a stabilita poskytovatele
- Bezpečnostní výhody:
  - SLA
  - Zajištění drahých bezpečnostních služeb (zálohování, incident management)
  - Sdílení drahých technologií (uživatel by si je sám nikdy nekoupil)

Cloud - specifikum

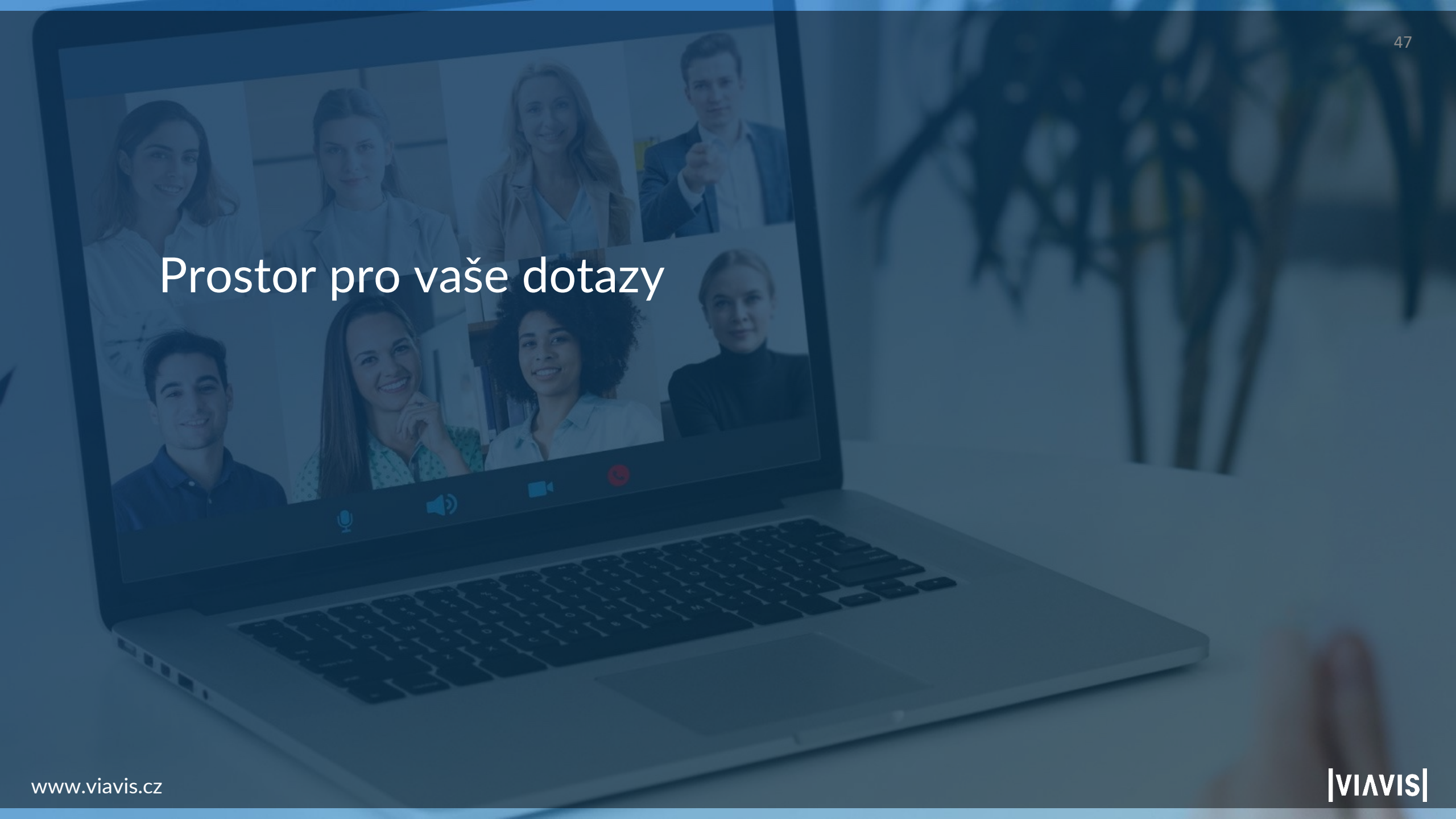
- Pokud uvažuji cloud – co bych měl řešit:
  - Kupuji si co – ne jak
  - Obsah služby
  - Výkon – ne konfiguraci
  - Rozsah služby – jak bude měřena účtována
  - SLA
  - Dostupnost
  - Business continuity
  - Management dat, výmaz dat
  - EXIT služby

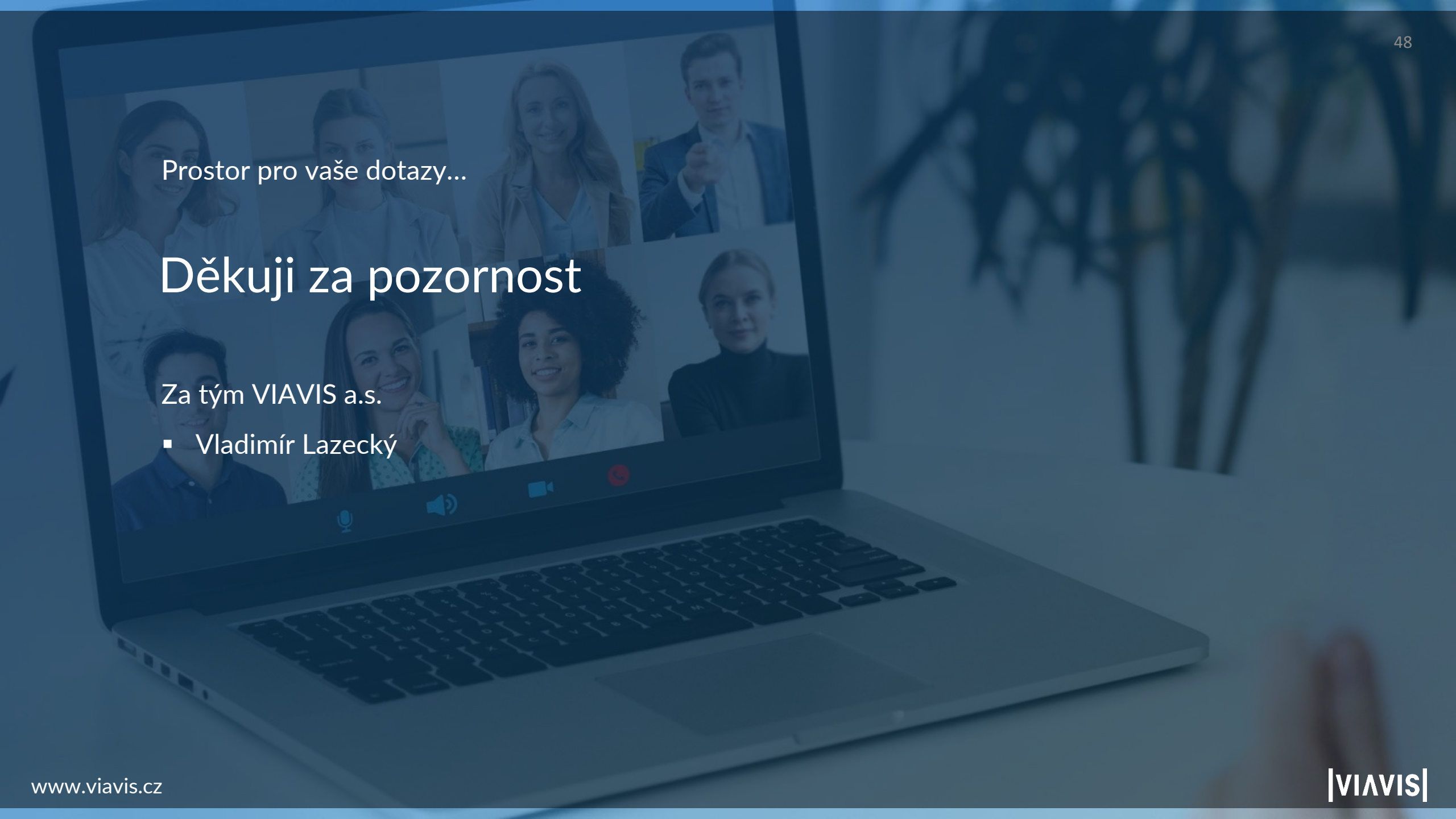
Vrstva služeb

- Služby poskytované IS – návrat ke katalogu služeb

- Forma poskytování:
  - Insourcing – realizace vlastními zaměstnanci
  - Outsourcing – realizace najatými subjekty

Prostor pro vaše dotazy





Prostor pro vaše dotazy…

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký