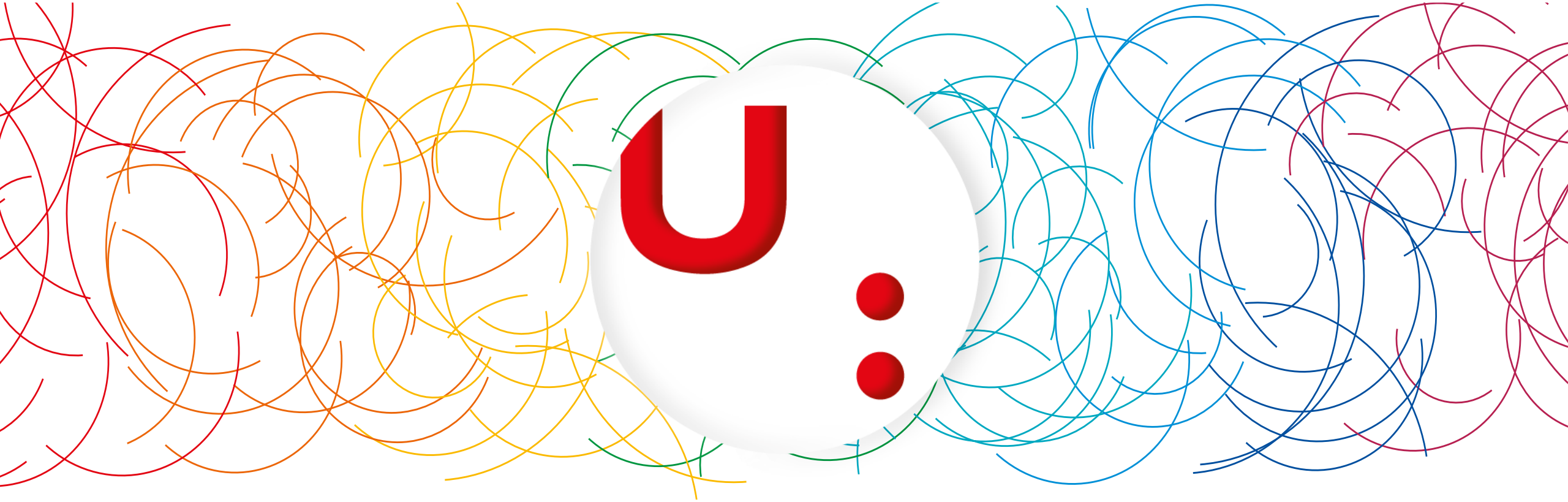


MFA a Analýza interních bezpečnostních rizik na Univerzitě Pardubice

Olga Klápšťová
Jiří Šafra

Něco málo o UPCE

7 fakult:

- Dopravní fakulta Jana Pernera
- Fakulta chemicko-technologická
- Fakulta ekonomicko-správní
- Fakulta elektrotechniky a informatiky
- Fakulta filozofická
- Fakulta restaurování
- Fakulta zdravotnických studií

- **CITS – opravdu centrální IT, všechny IT služby (včetně UKC a UK)**
- cca 7 000 studentů
- 1 150 zaměstnanců a cca 500 „dohodářů“
- ve správě péče o cca 4 000 PC a NTB (z toho 1 168 na učebnách fakult)

UNIVERZITA PARDUBICE

Proč hovořit o MFA ?

- Známé technologie a důvody pro MFA (nárůst využití elektronických identit, login a znalost hesla už není dostatečné zabezpečení, doplnit nějakou informaci danou vlastnictvím – mobil, token, …)
- Vyšší zabezpečení = zájem každé organizace
- Technická implementace – snadná
- Procesní implementace
  - V komerčním prostředí – obvykle jasné, direktivní
  - V akademickém prostředí – „výzva“ s nečekanými dopady

UNIVERZITA PARDUBICE

MFA na UPCE – pomalé začátky

- Banky
  - Směrnice Evropského parlamentu a Rady (EU) 2015/2366
  - Nařízení Komise (EU) 2018/389
- PEN testy září 2016 => IT UPCE začíná v roce 2017 řešit MFA ☺
  - Testování možností v úzkém kruhu IT administrátorů
    - Všichni v klidu… „ať si ajťáci hrají, když je to baví“
  - Nutná podmínka pro bezpečné přihlášení do Azure pro adminy
    - S Azure jsme v té době začínali
  - Nevyvíjíme si vlastní řešení
    - **Používáme řešení dostupné v rámci Azure**

UNIVERZITA PARDUBICE

Mezičas (2018-2021)

- Účinnost GDPR
- Diskuse, zda jsme OVM (…tak trochu ano, i když někdy ne ☺)
- Adopce cloudových technologií
- Několik projektů na kybernetickou bezpečnost
- Pandemie Covid-19
  - Násilná adaptace na online prostředí
  - Homeoffice
- Izolované nasazení MFA uživatelům, kteří se nebránili

Kybernetická bezpečnost (2021)

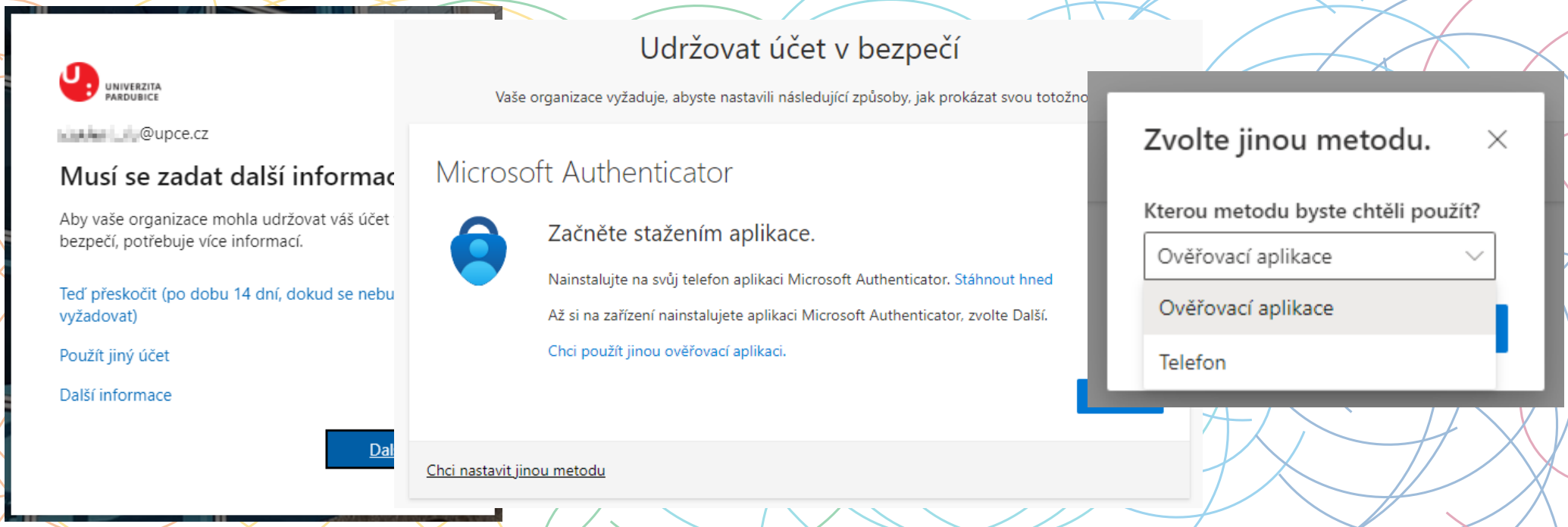
- Zanesena do interní legislativy (Směrnice č. 7/2021„Základní politika bezpečnosti informací - způsob zajištění kybernetické bezpečnosti na Univerzitě Pardubice“ Směrnice č. 7/2021)
- Oficiálně zastřešena
  - Manažerem kybernetické bezpečnosti
  - Výborem pro kybernetickou bezpečnost
- Na NÚKIB nahlášen první VIS
- Vhodný čas začít se zabývat plošným nasazením MFA - řízení změny

Záměr plošného nasazení MFA

- Nasazení MFA projednáno na VKB – 15. 9. 2021 a 15. 12. 2021
  - Shoda o potřebnosti nasazení MFA všem zaměstnancům
- Jednání vedení univerzity 13. 12. 2021
  - V zápise zmíněno pověření MKB koordinací nasazení
- Rozšířené vedení univerzity 17. 1. 2021
  - Informování představitelů fakult
- => pocit dostatečného mandátu ke konání

První pokus (a první odpor)

- Zapnutí tzv. *registration policy*
  - První přihlášení – výzva k zadání druhého faktoru



=> potřeba oficiálnější posvěcení

UNIVERZITA PARDUBICE

Druhý pokus

- Usnesení VKB 16. 3. 2022
  - pověření MKB zpracovat **opatření rektora** pro zabezpečení uživatelských účtů zaměstnanců pro nové i stávající uživatele
- Opatření vešlo v účinnost 8. 4. 2022
  - do 30. 4. budou mít všichni HPP registrovanou metodu zabezpečení
    - Registrace metody != vynucení při přihlášení
  - do 30. 9. budou mít totéž všichni DPP/Č
  - do 30. 4. bude upraven proces přijímání nových zaměstnanců s ohledem na MFA

UNIVERZITA PARDUBICE

Registrace metody MFA

- Každý si musí vybrat alespoň jednu z metod
  - zasílání potvrzovacích **SMS kódů**
  - využití **ověřovací aplikace** nainstalované na chytrém mobilním telefonu
  - využití **fyzického zařízení** (bezpečnostní token)
- Kdo má služební telefon s tarifem
  - automaticky nastaveno
- Kdo nemá, tomu v případě zájmu bude umožněno
  - registrovat soukromé číslo (GDPR) nebo
  - nainstalovat si autentikátor na soukromý telefon (ObZ)

UNIVERZITA PARDUBICE

Metody MFA

- Kdo nechce využít soukromé zařízení
  - Nemusí – nelze nutit (!)
    - Výslovný požadavek DPO
  - Může mu být pořízen služební telefon
  - Může mu být pořízen bezpečnostní token
    - Související náklady se hradí z prostředků útvaru, na kterém je příslušný zaměstnanec zaměstnán.
- Výběr metody koordinují vedoucí zaměstnanci

Informační kampaň

- Opatření rektora
  - Rozdělení povinností a odpovědností
- Servicedesk
  - Obrázkový návod a videonávod registrace metody
- Moodle
  - Informace o MFA a odkazy na všechny předchozí zdroje
- Wiki
  - Obecný popis, co je MFA a k čemu slouží

Informační kampaň

- Intranet
  - Informační stránky MKB
  - Oznámení o vydání opatření a odkazy na všechny předchozí zdroje
- Porada všech tajemníků
  - osobní představení
- Adresná emailová kampaň
- Osobní konzultace pro ty, kteří nesledují psané informace

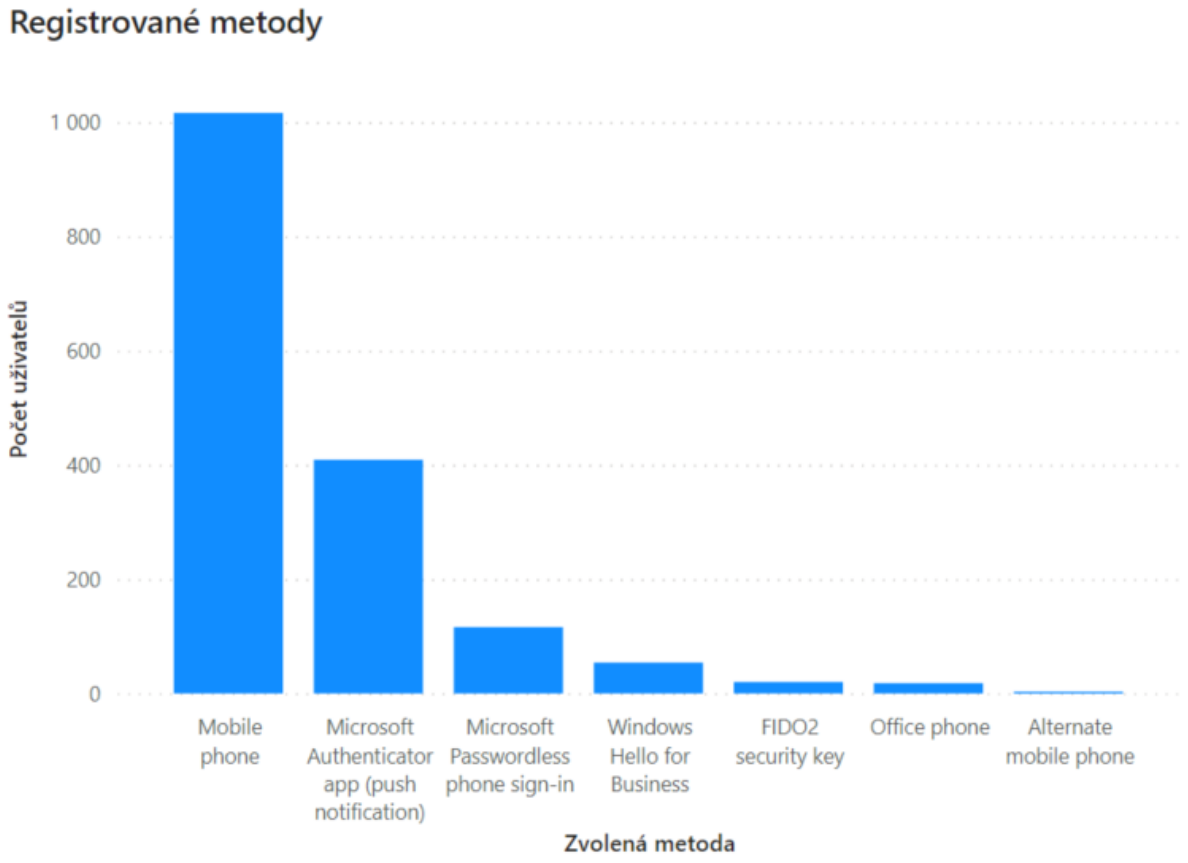
Aktuální stav (k 3. 11. 2022)

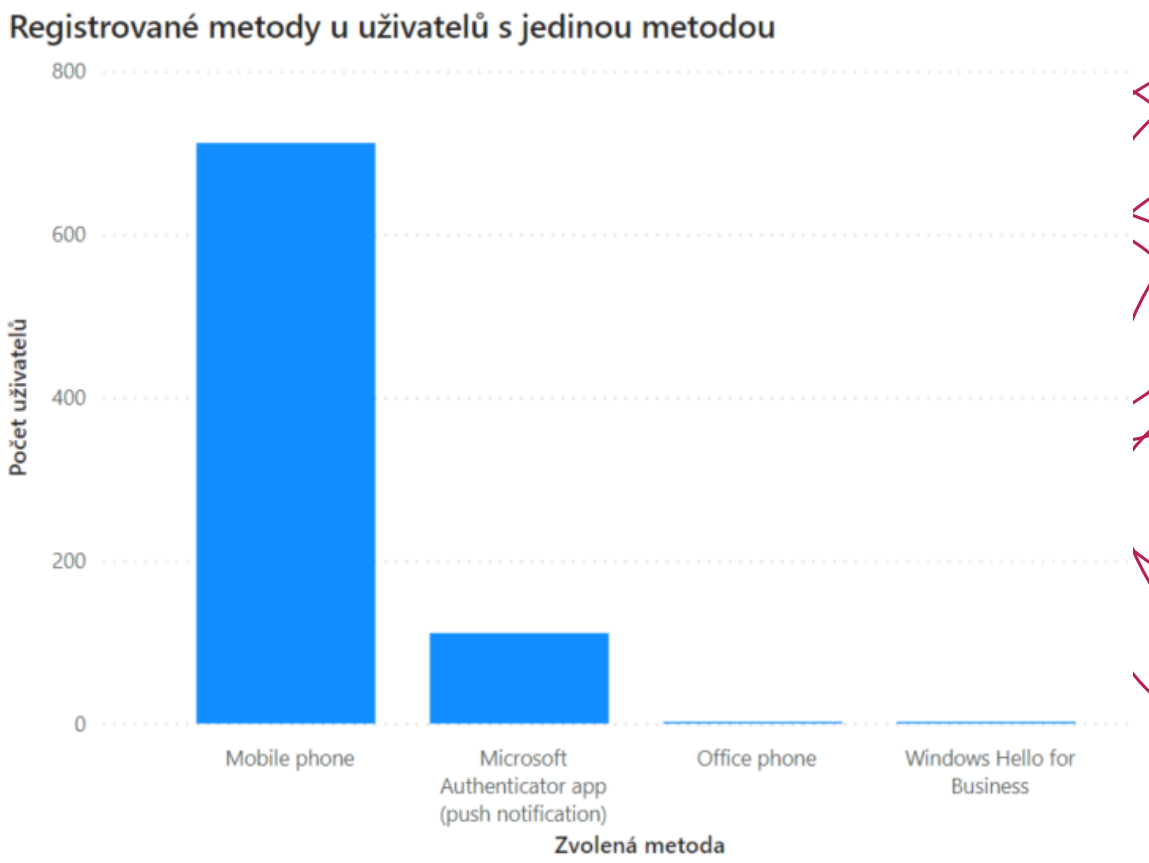
- Celkem máme cca 1150 zaměstnanců na HPP
  - Před vydáním opatření (8. 3.)
    - Metodu MFA zaregistrovalo cca 190 zaměstnanců
  - K termínu z opatření (30. 4.)
    - Metodu MFA zaregistrovalo cca 760 zaměstnanců
  - K 24. 5.
    - Metodu MFA zaregistrovalo cca 860 zaměstnanců

  => měsíc po termínu zbývalo zhruba 300 zaměstnanců
  - K 3.11. máme 1535 zaměstnanců (HPP + DPP), na HPP je jich 1139,
- Cca 95% zaměstnanců má tedy po ½ roce MFA nastaveno

UNIVERZITA PARDUBICE

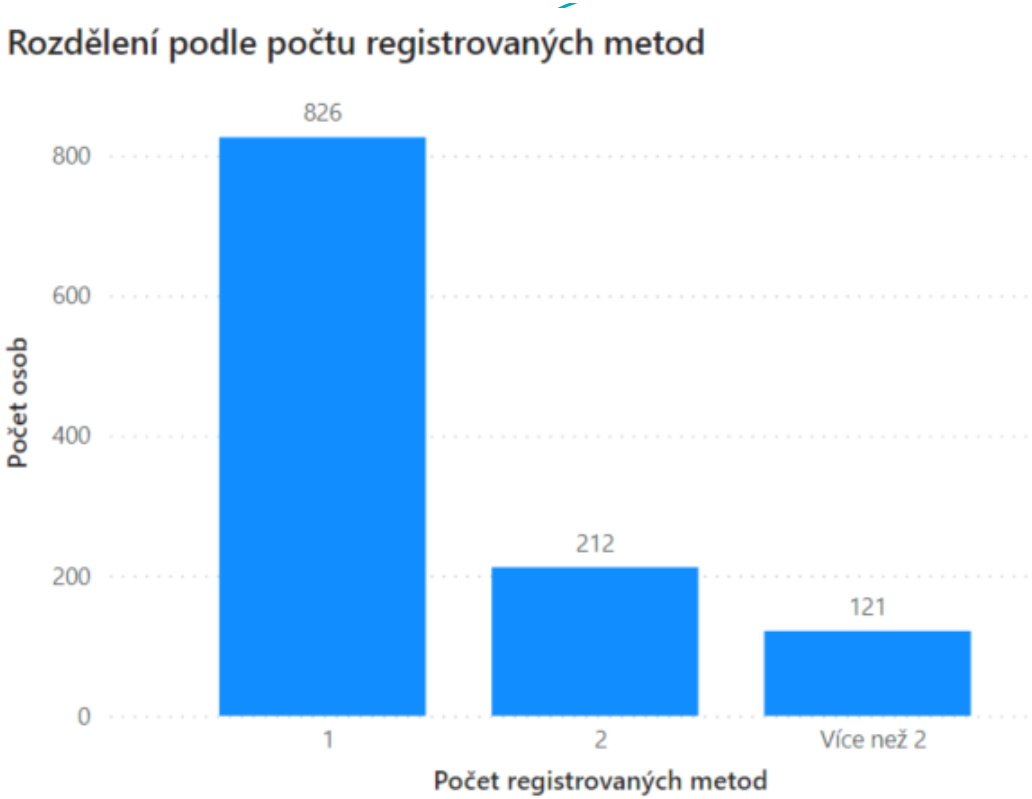
Aktuální stav





UNIVERZITA PARDUBICE

Aktuální stav



UNIVERZITA PARDUBICE

Další postup

- Zařazení další skupiny osob
  - Studenti
    - I bez kampaně si to někteří nastavují
- Rozšíření počtu zabezpečených systémů + sjednocení přihlašování
  - Dopad na intranet a obecně webové aplikace
    - Zapojení MS MFA do existujícího ekosystému
      - CAS, Shibboleth, Apache, Drupal (PHP CMS), ...

UNIVERZITA PARDUBICE

Správné pořadí kroků

1. MFA a zapnutí registrační politiky
2. Postupné vynucování při přihlášení
   - Office365
   - Mzdová agenda VEMA
   - VPN
   - Virtuální aplikace a desktopy
   - Aplikace přes Azure Application Proxy
3. Rozšiřovat množinu systémů, které budou MFA vyžadovat
   - Ideálně vše, co je VIS

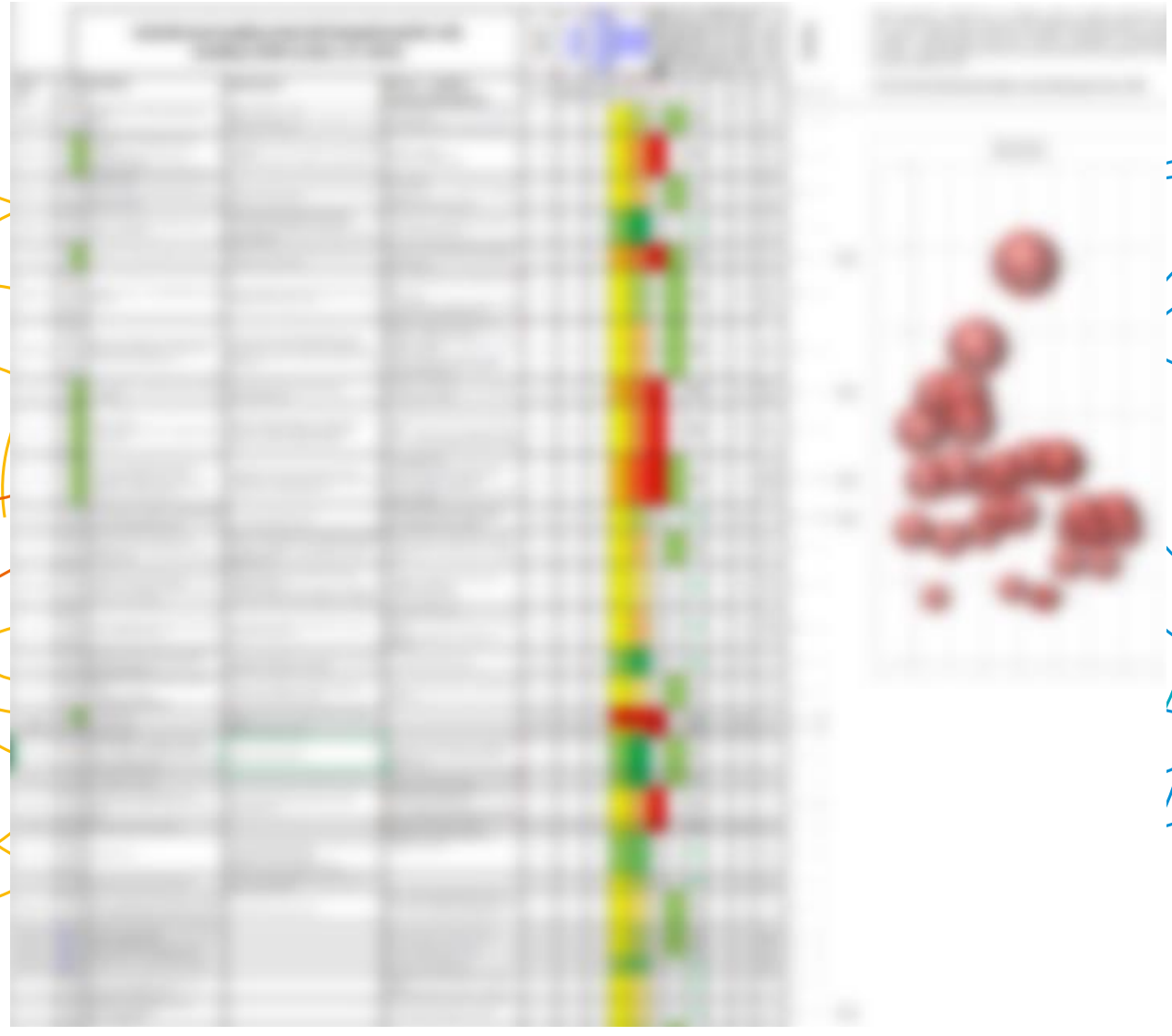
Implementace MFA – otevření téma KB – AIBR

- VKB – 15.6. 2022 – úkol připravit analýzu interních bezpečnostních rizik (AIBR)
  - zjištění slabých míst zabezpečení na straně koncových zařízení a uživatelských účtů
- Mimořádné zasedání VKB 29.6.
  - první verze AIBR s doporučením realizace všech doporučených opatření v souladu s povinnou legislativou
  - dopracování seznamu konkrétních opatření
- Zpracování následné detailní analýzy po fakultách
  - celé léto

AIBR – vstupní informace od MKB – 15 rizik

UNIVERZITA PARDUBICE

AIBR – během léta MKB – 30 rizik

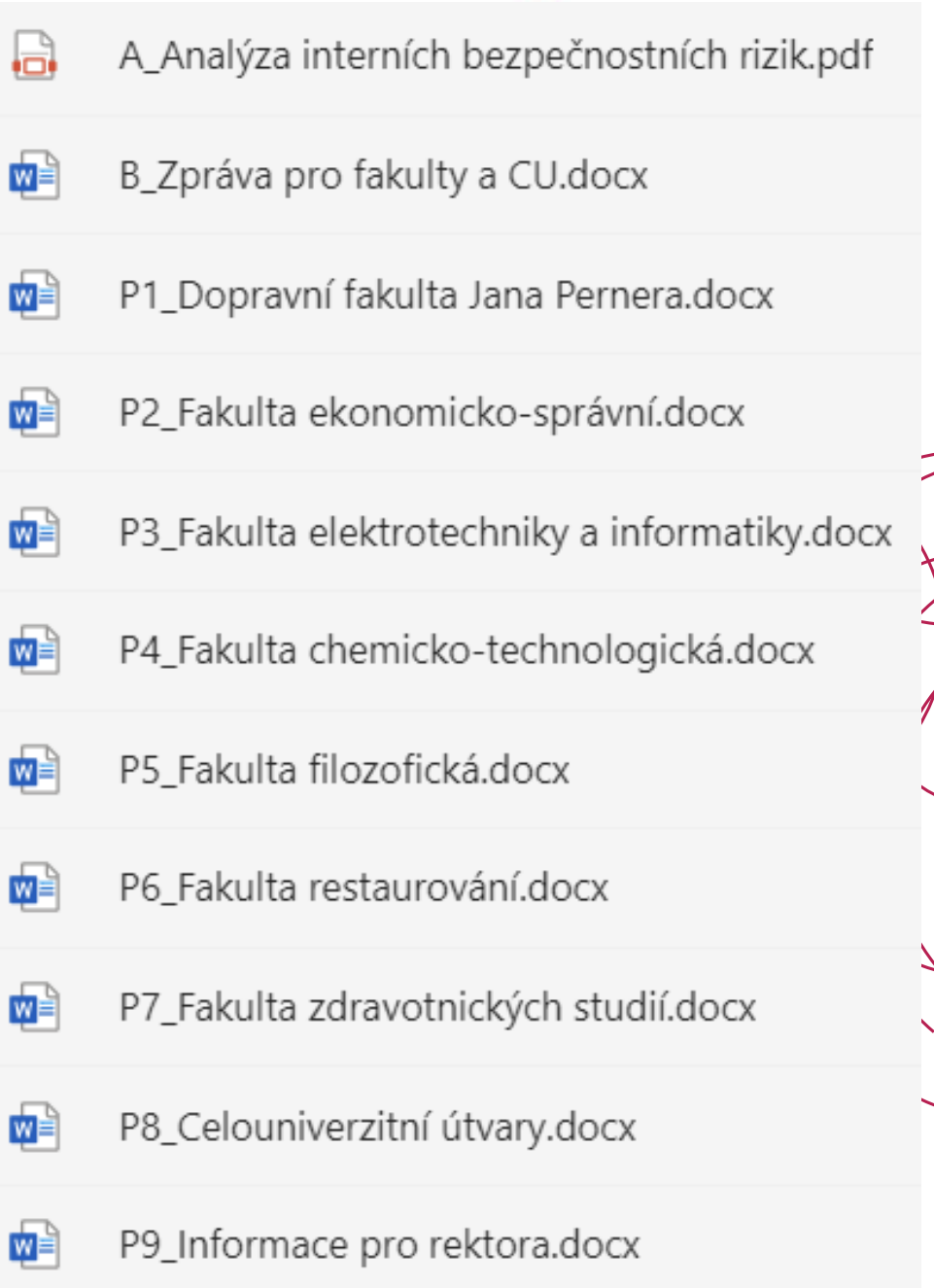


AIBR – 1. krok vybráno 9 rizik dle priority

UNIVERZITA PARDUBICE

Struktura AIBR

- Obecný dokument AIBR
- Informační zpráva pro fakulty
- Dílčí a velmi konkrétní zprávy o fakultách
- Zpráva o CÚ
- Informace pro rektora



Závěry fakultám – vysoká rizika

Položka	Zkrácený název rizika	Výše rizika (1-64)
4	**Uživatelé při běžné práci pracují s admin právy v operačním systému**	32
Ohrožení	Uživatelé mají oprávněný přístup do kritických IT služeb, k osobním údajům a dalším agendám, jsou důvěryhodnou součástí sítě a mají práva na rozličné operace s daty aplikací. Tím, že na svém HW prostředku zbytečně a nevědomky umožňují veškerým instalovaným, někdy zastaralým SW, škodlivým odkazům v poště, nebo na internetu ovládnout svůj počítač ať už vědomě, či z neznalosti, stávají se zbytečně nástrojem útočníka s velmi silnými právy.	
Opatření	Maximálně omezit používání administrátorských práv na zařízeních, kde to není nutné.	
Konkrétní řešení a kroky	CITS provede opakovanou revizi přidělených administrátorských práv na fakultě a mimo již evidované výjimky budou administrátorská práva postupně odebrána. Ze strany vedení fakulty by bylo vhodné informovat o tomto kroku vedoucí kateder. V případě, že uživatel bude potřebovat administrátorská práva, může požádat o tyto práva přes ServiceDesk – služba „Instalace a nastavení software“. Tato práva pak lze přidělit podle konkrétní situace.	
9	**Zastaralá a nespravovaná zařízení nelze zabezpečit a vyskytují se v interní síti**	38
Ohrožení	Nespravovaná nebo zastaralá zařízení trpí zranitelnostmi, nejsou řízeny bezpečnostními politikami, jsou snadno napadnutelná a jsou přímou hrozbou pro ostatní zařízení v síti. S přihlášeným uživatelem pak mají příslušná práva na serverové IT služby.	
Opatření	Tato zařízení učinit spravovanými dle standardních konfigurací, nebo je izolovat z interní sítě a používat je jen pro jednoúčelovou službu	
Řešení	Technici CITS budou postupně kontaktovat jednotlivé uživatele s těmito zařízeními a provedou reinstalaci nebo oddělení zařízení do izolované sítě, která umožní nezbytné služby, a kde tato zařízení nebudou potencionální hrozbou pro organizaci. V zásadě se jedná o jednotky zařízení.	

Závěry fakultám – vysoká rizika

Položka	Zkrácený název rizika	Výše rizika (1-64)
7	**Zastaralé a neaktualizované aplikace na počítačích**	32
Ohrožení	Na počítačích jsou instalovány neaktualizované a zastaralé SW, které jsou zranitelné a tudíž snadno zneužitelné škodlivým kódem. S přihlášeným uživatelem pak mají příslušná práva na IT služby.	
Opatření	Monitorovat stav koncových stanic a striktně vyžadovat soulad v oblasti aplikace bezpečnostních záplat.	
Řešení	CITS provede opětovnou kontrolu stavu aktuálnosti nainstalovaného SW, následně proběhne aktualizace SW nebo jeho odinstalování (často jsou některé SW instalovány zbytečně, nebo zůstávají nainstalovány z minulosti bez aktuální potřeby). V případě, že toto nebude možné, bude dále hledáno řešení k nápravě a konzultováno s vedením fakulty.	

Závěry fakultám – střední rizika

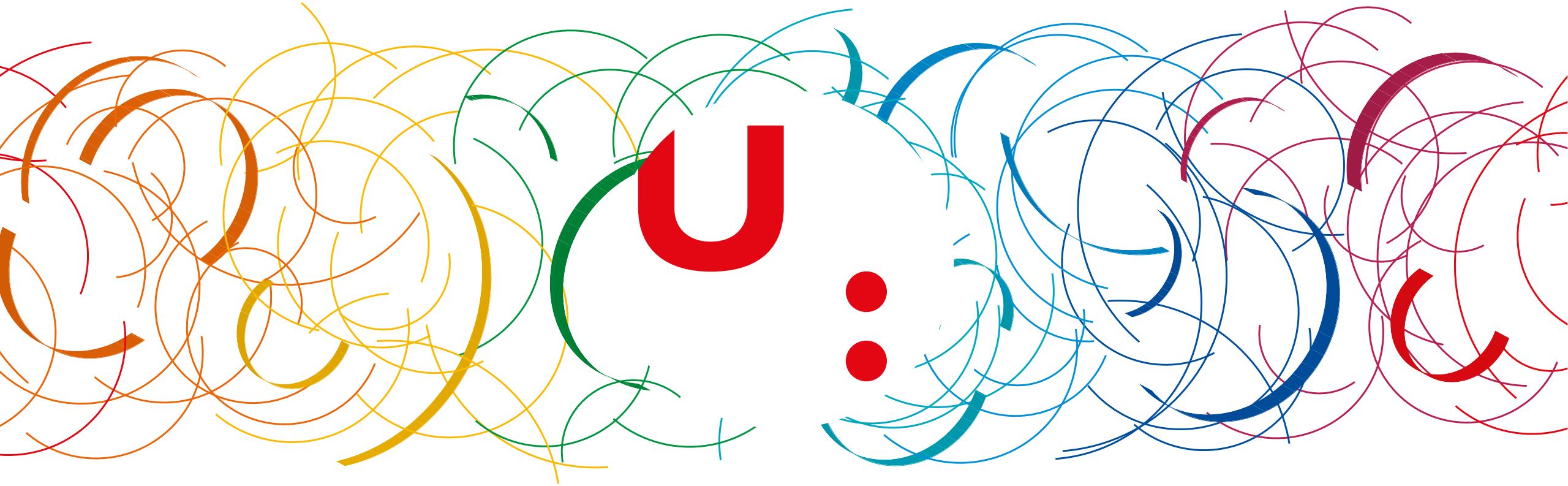
Položka	Zkrácený název rizika	Výše rizika (1-64)
5	**Zabezpečení vzdáleného přístupu k interním službám UPCE**	27
Ohrožení	Trvalé připojení z externí sítě, z domova na pracovní počítač uživatele ve vnitřní síti prostřednictvím SW třetích stran nelze kontrolovat. Pracovní počítač není zabezpečený server poskytující služby.	
Opatření	Eliminovat provoz ovládacích SW typu TeamViewer, AnyDesk, … Dále probíhá revize všech servisních VPN.	
Řešení	CITS provede analýzu používání těchto SW. Tento typ SW je nutné maximálně eliminovat a vzdálená připojení umožnit pouze ze známých zařízení a schváleným způsobem.	

Položka	Zkrácený název rizika	Výše rizika (1-64)
6	**Zabezpečení přihlašovacích údajů a dat uživatelů**	23
Ohrožení	Uživatelé mohou používat zastaralé protokoly, které neumožňují bezpečné přihlašování uživatelů. Automatické přeposílání e-mailové komunikace zaměstnanců mimo organizaci ohrožuje bezpečnost těchto dat.	
Opatření	Zastaralé protokoly jsou v organizaci maximálně eliminovány. Automatické přeposílání e-mailové komunikace by mělo být ponecháno pouze v případech externistů a studentů.	
Řešení	Zastaralé autentizační protokoly (tzv. „Legacy protokoly“), byly v našem tenantu upce.cz ze strany poskytovatele cloudových služeb ukončeny k **17.10.2022**. Po tomto datu již nefungují, a uživatelé kteří je dosud používali, si museli svá zařízení překonfigurovat správným způsobem. Automatické přeposílání e-mailové komunikace není doporučeno a bude povoleno v odůvodněných případech se souhlasem nadřízeného. Toto přeposílání nebude možné pro skupinu „VIP uživatelů“ (všichni vedoucí pracovníci, pracovníci na významných pozicích, pracovní pozice pracující s důvěrnými a citlivými daty, apod …) Dále je potřeba dokončit registraci MFA u uživatelů, kteří tak již dosud neučinili.	

UNIVERZITA PARDUBICE

Závěrem

- AIBR je Pandořina skříňka – MFA otevřelo další témata KB
- Musí existovat centrální IT schopné zajistit následné služby
- Nezbytná podpora vedení
- Je důležité najít správnou chvíli pro tyto kroky
  - (vnější situace, nové vedení, …), ale nelze odkládat
- Nutné vytrvat, být důslední v realizaci opatření a umět změny řídit
- Klíčová je komunikace, osvěta
  - různé kanály, různé formy
- Plnit sliby a termíny na obou stranách



Děkuji za pozornost