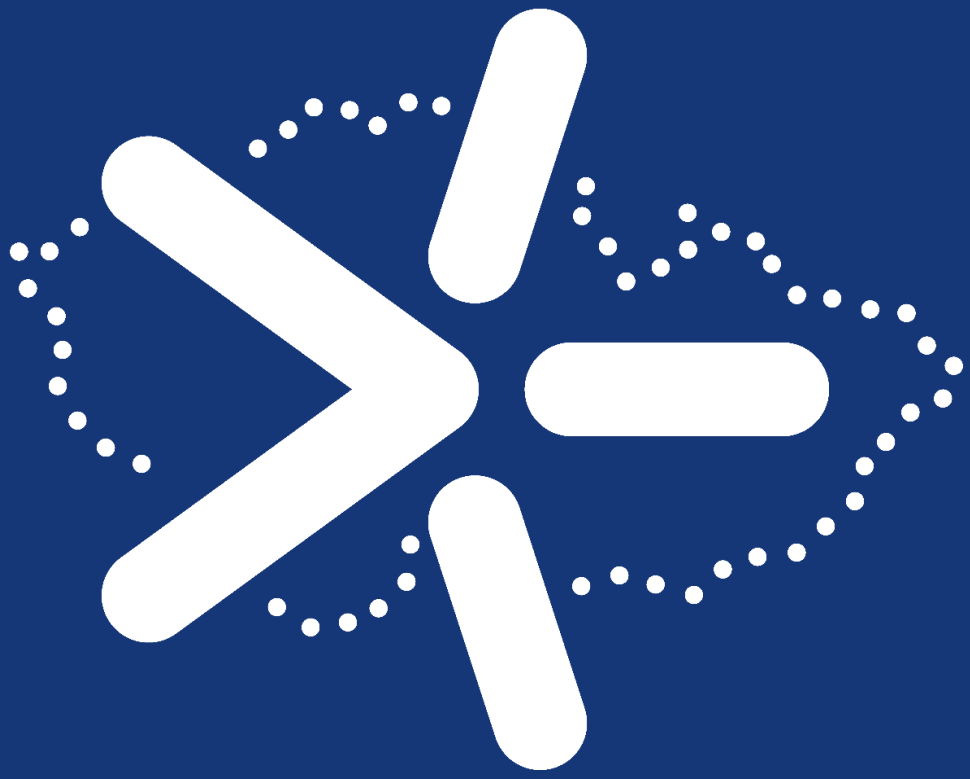

DOPORUČENÍ PRO ZABEZPEČENÍ KOLABORATIVNÍ PLATFORMY, VČETNĚ DOPORUČENÍ PRO JEJÍ POKROČILÉ NASTAVENÍ

Výstup č. 1

Popis výstupu č. 1 za Janáčkovu akademii múzických umění

Janáčkova akademie múzických umění

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

Financováno Evropskou unií
NextGenerationEU

Obsah

Financováno Evropskou unií
NextGenerationEU

Financováno Evropskou unií
NextGenerationEU

Anotace výstupu

Výstup č. 1 za Janáčkovu akademii múzických umění popisuje implementaci jednotlivých doporučení pro zabezpečení kolaborativní platformy, včetně doporučení pro její pokročilé nastavení, jež byly zpracovány v rámci výstupu č. 1 pracovní skupinou PS2. Jednotlivá doporučení jsou publikována na adrese https://muni.cz/go/M365Security. V popisu výstupu je tak uvedeno, která doporučení:

- byla implementována, vč. upřesnění způsobu nebo rozsahu nasazení,
- nebyla implementována,
- termín kdy budou doporučení implementována,
- důvod, proč doporučení nebylo možné implementovat.

Popis výstupu

Obecná opatření

Publikujte technické kontakty a nápovědu

Publikujte technické kontakty a nápovědu

☒ Ověřena existence a doručitelnost mailových kontaktních adres podle RFC

☐ Publikovány informace v security.txt

☒ Zaveden technický kontakt pro podporu ze strany Microsoftu

☒ Zaveden technický kontakt pro podporu koncových uživatelů

☐ Zavedeny informace o ochraně dat pro koncové uživatele

☐ Zjištěny a dostupné technické kontakty v rámci organizace

☐ Zjištěny a dostupné technické kontakty mimo organizaci

Ověřte nastavení auditního logování

Ověřte nastavení auditního logování

☒ Auditní logování nastaveno

Financováno Evropskou unií
NextGenerationEU

Nastavte umístění pro uchování a zpracování dat tenantu

Nastavte umístění, kde budou uchovávána a zpracovávána data tenantu

☒ Umístění nastaveno

- s výjimkou zpráv Yammeru/Viva Engage.

Nastavte schvalování přístupu MS k datům tenantu

Nastavte schvalování přístupu MS k datům tenantu

☒ Customer lockbox nastaven

- Nebudeme nastavovat

Ochrana identit – prevence

Upravte branding přihlašování

Upravte branding přihlašování (Azure AD)

☐ Upravena přihlašovací stránka do vizuálu organizace

Vytvořte přímé odkazy na tenant a zapamatovatelná přesměrování

Používejte odkazy směřující na váš tenant a připravte zapamatovatelná přesměrování

☒ Linky a přesměrování nastaveny

Nastavte adresu odesílatele systémových notifikací

Nastavte adresu odesílatele systémových notifikací

☒ Nastavena vlastní doména pro zasílání systémových notifikací

Financováno Evropskou unií
NextGenerationEU

Upravte branding prostředí MS 365

Upravte branding prostředí MS 365

☐ Nastaven vizuál prostředí MS 365

Oddělte účty správců a nastavte přesměrování admin schránek

Oddělte admin a uživatelské účty správců a nastavte přesměrování admin schránek

☒ Rozhodnuto, která oprávnění mohou/nemohou dostávat běžné účty

☒ Vytvořeny účty pro správce oddělené od běžných provozních účtů

- S výjimkou účtů fakultních správců, kteří mají přidělena jen vybraná zvýšená oprávnění

☒ Nastaveno MFA (kromě specifikovaných výjimek)

- Pro centrální správce a fakultní správce se zvýšenými oprávněními. Pro běžné uživatele nevyžadováno.

☒ Nastavena přesměrování pro správcovské účty

- Pro dedikované účty

☒ Přidělena minimální nezbytná oprávnění

- Oprávnění zrevidována, odebrána nadbytečná oprávnění

☒ Nastaven proces revize účtů se zvýšeným oprávněním

Vytvořte záchranné účty globálních administrátorů

Vytvořte záchranné účty globálních administrátorů

☐ Účty vytvořeny a otestovány

☐ Přihlašovací údaje uloženy a zajištěna dostupnost

☐ Nastaven proces kontroly dostupnosti přihlašovacích údajů a funkčnosti záchranných účtů

Nevytvářejte anonymní účty/účty se sdíleným heslem

Nevytvářejte anonymní účty, účty se sdíleným heslem

☒ Nastavena pravidla, kdy je možné využívat anonymní účty/účty se sdíleným heslem

☒ Provedena revize existujících účtů, jejich nahrazení vhodnějšími nástroji

Financováno Evropskou unií
NextGenerationEU

Nastavte omezení pro vytváření guestů a oprávnění guestů

Nastavte omezení pro vytváření guestů a oprávnění guestů

☒ Nastaveno oprávnění pro vytváření guestů a oprávnění guestů

Zakažte běžným uživatelům přístup do Azure AD portálu

Zakažte běžným uživatelům přístup do Azure AD portálu

☒ Přístup pro uživatele do Azure AD portálu zakázán

- Nebylo nastaveno, uživatelé potřebují přístup kvůli registraci aplikací

Zakažte běžným uživatelům vytvářet další Azure AD tenanty

☒ Běžní uživatelé mají zakázáno vytvářet další Azure AD tenanty

Zakažte běžným uživatelům připojovat zařízení do Azure AD

Zablokujte možnost připojení zařízení běžných uživatelů do Azure AD

☒ Zablokována možnost připojení zařízení běžných uživatelů do Azure AD

Nastavte synchronizaci hashí hesel

Nastavte synchronizaci hashí hesel

~~☐ Zkontrolovány prerekvizity~~

~~☐ Spuštěna synchronizace~~

- využíváme IdP, v AD nemáme správná hesla

Zrušte expiraci uživatelských hesel (Password expiration policy)

Zrušte expiraci uživatelských hesel

☒ Expirace zrušeny

Blokujte snadno prolomitelná hesla

Blokujte snadno prolomitelná hesla

☐ Zablokována hesla podle global banned password list

- pouze v audit mode Metody ověřování – Centrum pro správu Azure Active Directory

Financováno Evropskou unií
NextGenerationEU

- jen pro cloudové účty

~~☐ Nastaven custom banned password list~~

Povolte společnou registraci ověřovacích údajů pro vícefaktorové přihlašování a samoobslužný reset hesel

Povolte společnou registraci ověřovacích údajů pro vícefaktorové přihlašování a samoobslužný reset hesel (Combined security information registration)

☒ Společná registrace pro MFA a SSPR povolena

Omezte/zakažte základní ověřování

Omezte/zakažte základní ověřování

☐ Základní ověřování zakázáno

☐ Základní ověřování omezeno

Nastavte samoobslužný reset hesel

Nastavte samoobslužný reset hesel

~~☐ Samoobslužný reset hesel nastaven~~

- běžný uživatel řeší pře IS MU, cloud účty mají zakázáno

Povolte/vynuťte vícefaktorové ověřování

Povolte/vynuťte vícefaktorové ověřování

☐ MFA nastaveno

- nastaveno pouze pro cloudové admin účty, ostatní řešeny v IdP, s výjimkou účtů se zvýšenými oprávněními dobrovolné

Omezte registraci a schvalování přístupu aplikací

☐ Rozhodnuto o pravidlech pro povolení enterprise aplikací a registrace aplikací

- Pravidla připravena a připravena pro nasazení, připraven skript pro odebrání nepoužívaných souhlasů a souhlasů u nepoužívaných aplikací, nasazení 05/2024

Financováno Evropskou unií
NextGenerationEU

☐ Nastavena pravidla pro registrace nových aplikací

☐ Nastavena pravidla pro udělování souhlasů pro enterprise aplikace

☐ Zrevidovány existující enterprise a registrované aplikace

Ochrana poštovní komunikace

Autentizujte zprávy, zabraňte podvržení, budujte reputaci domén

Autentizujte zprávy, zabraňte jejich podvržení, buduje reputaci svých domén

☒ Nastaveny SPF, DKIM, DMARC pro všechny domény organizace

Zpřesněte autentizaci odesílajících systémů při využití GW/Relay

Zpřesněte autentizaci odesilatelů při využití Gateway/Relay

☒ Nastaven Enhanced Filtering for Connectors/Skip listing pro všechny přeposílající systémy

Ověřte, že máte povoleno auditování mailboxů

Ověřte, že máte povoleno auditování mailboxů

☒ Auditování mailboxů povoleno

Nastavte podle potřeby politiky pro ochranu pošty

Nastavte politiky pro ochranu pošty

☒ Politiky pro ochranu pošty nastaveny

Nastavte upozorňování uživatelů na zprávy podezřelých odesílatelů

☒ Upozorňování na zprávy podezřelých odesilatelů nastaveno

☒ Upozorňování na nové/občasné odesilatele

Nastavte upozorňování na spustitelné přílohy zpráv nebo je zablokujte

☒ Upozorňování/zablokování nastaveno

Omezte počet odeslaných zpráv za jednotku času

Financováno Evropskou unií
NextGenerationEU

☒ Omezení počtu odeslaných zpráv nastaveno

Omezte externí přesměrování zpráv

☐ Omezení externího odesílání nastaveno

- Nenastaveno, nasazení této politiky bude řešeno v příštím roce

Nasaďte doplněk pro hlášení (ne)vyžádané pošty

☒ Doplněk pro hlášení pošty nastaven

Porovnejte aktuální nastavení s přednastavenými politikami dle Microsoftu

~~☐ Provedeno srovnání s doporučeními od Microsoftu~~

Nastavení monitoringu a reakcí – identity

Nastavte sledování a reakce na podezřelá přihlášení a ohrožené účty

☒ Nastaven proces pro sledování podezřelých přihlášení a ohrožených účtů a reakce na ně

Sledujte bezpečnostní upozornění

☐ Nastaveno sledování a reakce na bezpečnostní upozornění

- v přípravě

Provádějte revize účtů se zvýšenými oprávněními

☒ Revize nastaveny[1]

Ověřujte dostupnost a funkčnost záchranných účtů

☐ Kontroly záchranných účtů nastaveny

Nastavení monitoringu a reakcí – pošta

Nastavte procesy revizí pro poštu

Revidujte nahlášenou (ne)vyžádanou poštu

☐ Proces revizí nastaven

[1] https://servicedesk-muni.atlassian.net/wiki/spaces/services/pages/360087753/Internal+Documentation+-+Microsoft+Office+365#P%C5%99%C3%ADjde-nebo-odejde-zam%C4%9Bstnanec-CIT-z-MU%2C-pot%C5%99ebuje-opr%C3%A1vn%C4%9Bn%C3%AD-pro-spr%C3%A1vu-O365

Financováno Evropskou unií
NextGenerationEU

- v přípravě

Revidujte poštovní karanténu

☒ Proces revizí nastaven

Revidujte povolené/blokované odesilatele spoofovaných zpráv

☐ Proces revizí nastaven

- v přípravě

Nastavte proces reakce na phishingové kampaně

Vyšetřování phishingových zpráv (draft)

☐ Proces pro vyšetřování phishingových kampaní nastaven

- v přípravě

Financováno Evropskou unií
NextGenerationEU