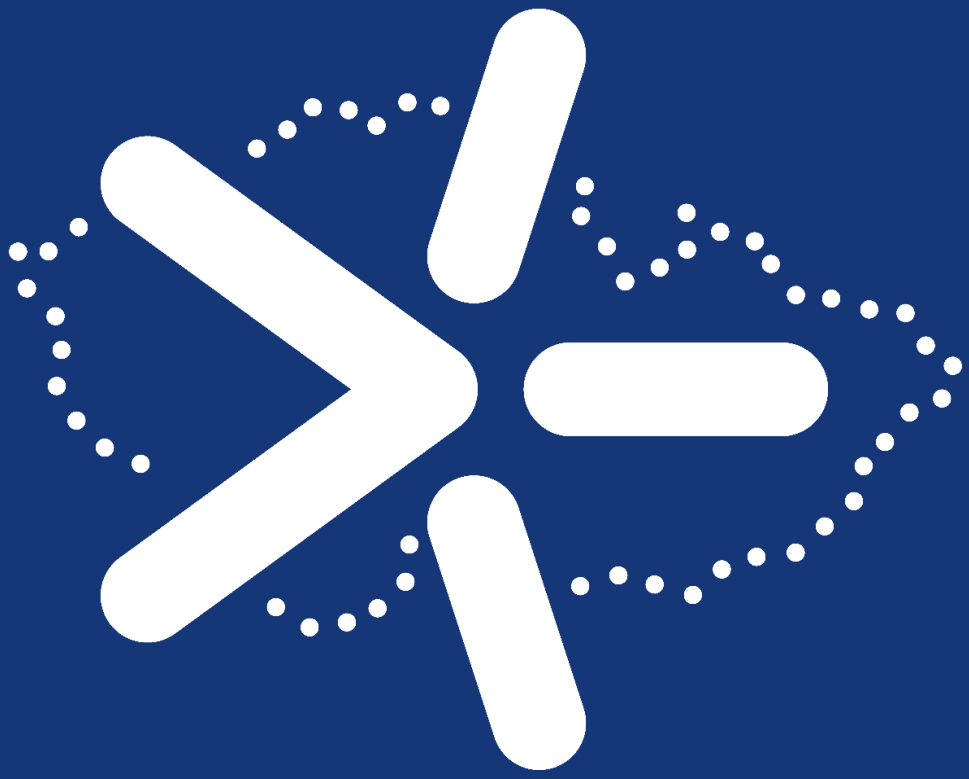

VÝSTUP Č. 2 ČZU

Přijetí a aplikace doporučení z vypracované technické zprávy z průběhu implementace.

Cíl: Realizace zvoleného způsobu zabezpečení kolaborativní platformy pro potřeby zajištění distančního vzdělávání a implementace doporučených opatření v nově nasazených i stávajících platformách.

Pracovní skupina 3 NPO-C2
vlachynsky@rektorat.czu.cz

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

Obsah

Anotace výstupu

V rámci projektu NPO-C2 byly řešiteli pracovní skupiny PS6 definovány a implementovány bezpečnostní doporučení a standardy pro zvýšení zabezpečení prostředí Microsoft365 z ostatních vysokých škol.

O spolupráci s PS6 požádaly Janáčkova akademie múzických umění a Slezská univerzita. V samostatných kapitolách Výstupu č. 19 NPO-C2 je popsána spolupráce s těmito školami a technická opatření, která byla těmto školám implementována.

V rámci tohoto dílčího výstupu pro potřeby České zemědělské univerzity budou jednotlivá opatření popsána a pro případné nasazení a implementace do vnitřního prostředí bude vytvořen checklist konkrétních doporučení. Tento checklist bude dále zpřístupněn konkrétním pracovištím pro potřeby vnitřního auditu a případným implementacím do prostředí.

Obecná opatření

Publikujte technické kontakty a nápovědu

Publikujte technické kontakty a nápovědu

- ☐ Ověření existence a doručitelnost mailových kontaktních adres podle RFC
- ☐ Zavedení technického kontaktu pro podporu ze strany Microsoftu
- ☐ Zavedení technického kontaktu pro podporu koncových uživatelů
- ☐ Zavedení informací o ochraně dat pro koncové uživatele

Ověřte nastavení auditního logování

Ověřte nastavení auditního logování

- ☐ Ověření auditního logování

Ochrana identit – prevence

Nastavte adresu odesílatele systémových notifikací

Nastavte adresu odesílatele systémových notifikací

- ☐ Nastavení vlastní adresy pro zasílání systémových notifikací

Oddělte účty správců a nastavte přesměrování admin schránek

Oddělte admin a uživatelské účty správců a nastavte přesměrování admin schránek

- ☐ Rozhodnutí, která oprávnění mohou/nemohou dostávat běžné účty
- ☐ Vytvoření účtů pro správce oddělené od běžných provozních účtů
- ☐ Nastavení MFA (kromě specifikovaných výjimek)
- ☐ Nastavení přesměrování pro správcovské účty
- ☐ Přidělení minimálních nezbytných oprávnění
- ☐ Nastavení procesu revize účtů se zvýšeným oprávněním

Nevytvářejte anonymní účty/účty se sdíleným heslem

Nevytvářejte anonymní účty, účty se sdíleným heslem

NPO-C2 PS3

☐ Nastavení pravidla, kdy je možné využívat anonymní účty/účty se sdíleným heslem

☐ Provedení revize existujících účtů, jejich nahrazení vhodnějšími nástroji

Nastavte omezení pro vytváření guestů a oprávnění guestů

Nastavte omezení pro vytváření guestů a oprávnění guestů

☐ Nastavení oprávnění pro vytváření guestů a oprávnění guestů

Zakažte běžným uživatelům přístup do Azure AD portálu

Zakažte běžným uživatelům přístup do Azure AD portálu

☐ Zakázání přístupu pro uživatele do Azure AD portálu

Zakažte běžným uživatelům vytvářet další Azure AD tenanty

☐ Zakázání pro běžné uživatele vytvářet další Azure AD tenanty

Zakažte běžným uživatelům připojovat zařízení do Azure AD

Zablokujte možnost připojení zařízení běžných uživatelů do Azure AD

☐ Zablokování možnosti připojení zařízení běžných uživatelů do Azure AD

Nastavte synchronizaci hash hesel

☐ Hesla jsou do Entra ID nahrávána z UIS/či jiných doporučených IdM systémů

Zrušte expiraci uživatelských hesel (Password expiration policy)

Zrušte expiraci uživatelských hesel

☐ Zrušení expirace

Blokujte snadno prolomitelná hesla

Blokujte snadno prolomitelná hesla

Metody ověřování – Centrum pro správu Azure Active Directory.

☐ Zablokování hesel podle global banned password list

☐ Nastavení 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)

☐ Povolení společné registrace pro MFA a SSPR

Omezte/zakažte základní ověřování

Omezte/zakažte základní ověřování

☐ Zakázání základní ověřování

Nastavte samoobslužný reset hesel

Nastavte samoobslužný reset hesel

☐ Nastavení samoobslužného resetu hesel

Upravte nastavení autentizačních metod pro MFA a SSPR

☐ Nastavení dostupné metody pro MFA a SSPR

Omezte registraci a schvalování přístupu aplikací

☐ Nastavení pravidla pro registrace nových aplikací

Ochrana poštovní komunikace

Autentizujte zprávy, zabraňte podvržení, budujte reputaci domén

Autentizujte zprávy, zabraňte jejich podvržení, buduje reputaci svých domén

☐ Nastavení SPF, DKIM, DMARC pro všechny domény organizace

Ověřte, že máte povoleno auditování mailboxů

Ověřte, že máte povoleno auditování mailboxů

☐ Povolení auditování mailboxů

Nastavte podle potřeby politiky pro ochranu pošty

Nastavte politiky pro ochranu pošty

☐ Nastavení politiky pro ochranu pošty

Nastavte upozorňování uživatelů na zprávy podezřelých odesílatelů

☐ Nastavení upozorňování na zprávy podezřelých odesilatelů

Nastavte upozorňování na spustitelné přílohy zpráv nebo je zablokujte

☐ Nastavení upozorňování/zablokování

Omezte počet odeslaných zpráv za jednotku času

☐ Omezení počtu odeslaných zpráv nastaveno

Nasaďte doplněk pro hlášení (ne)vyžádané pošty

☐ Nastavení doplňku pro hlášení pošty

Omezte externí přesměrování zpráv

☐ Nastavení omezení externího odesílání

Porovnejte aktuální nastavení s přednastavenými politikami dle Microsoftu

☐ Provedení srovnání s doporučeními od Microsoftu

Nastavení monitoringu a reakcí – identity

Nastavte sledování a reakce na podezřelá přihlášení a ohrožené účty

☐ Nastavení zasílání upozornění a reportů

☐ Nastavení procesu pro sledování podezřelých přihlášení a ohrožených účtů a reakce na ně

Sledujte bezpečnostní upozornění

☐ Nastavení sledování a reakce na bezpečnostní upozornění

Provádějte revize účtů se zvýšenými oprávněními

☐ Nastavení revize účtů se zvýšenými oprávněními

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

☐ Nastavení procesu revizí pro (ne)vyžádanou poštu

Revidujte poštovní karanténu

☐ Nastavení procesu revizí pro poštovní karanténu

Nastavte proces reakce na phishingové kampaně

Vyšetřování phishingových zpráv (draft)

☐ Nastavení procesu pro vyšetřování phishingových kampaní

Zpřesněte autentizaci odesílajících systémů při využití GW/Relay

Zpřesněte autentizaci odesilatelů při využití Gateway/Relay

☐ Nastavení Enhanced Filtering for Connectors/Skip listing pro všechny přeposílající systémy

Nastavení monitoringu a reakcí – pošta

Nastavte procesy revizí pro poštu

Revidujte nahlášenou (ne)vyžádanou poštu

☐ Nastavení procesu revizí

Revidujte poštovní karanténu

☐ Nastavení procesu revizí

Revidujte povolené/blokované odesilatele spoofovaných zpráv

☐ Nastavení procesu revizí

Nastavte proces reakce na phishingové kampaně

Vyšetřování phishingových zpráv (draft)

☐ Nastavení procesu pro vyšetřování phishingových kampaní