VÝSTUP Č. 5

Doporučení pro zabezpečení kolaborativní platformy, včetně doporučení pro její pokročilé nastavení

Akceptace a přizpůsobení výsledků činnosti pracovní skupiny pro potřeby VŠTE

Vypracování plánu implementace a integrace kolaborativní platformy pro VŠTE a jeho realizace

Pracovní skupina 3 NPO-C2 a tým VŠTE

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

Obsah

Zabezpečení emailových služeb VŠTE

Charakteristika dokumentu

V rámci projektu NPO-C2 byly řešiteli pracovní skupiny PS2 definovány bezpečnostní doporučení a standardy pro e-mailovou komunikaci, které by měly univerzity a vysoké školy splňovat. Na Vysoké škole technické a ekonomické v Českých Budějovicích, dále jen VŠTE, jsou v průběhu projektu NPO prováděny změny v nastavení zabezpečení e-mailu odpovídající těmto doporučením. Přehled a popis již realizovaných a plánovaných změn je předmětem tohoto dokumentu. Je třeba upozornit, že ke změnám dochází průběžně a tento dokument zachycuje stav změn v průběhu a ke konci roku 2023.

Nejprve si na začátek v hrubých rysech představíme topologii e-mailových služeb na VŠTE. Následně pak shrneme změny a doporučení, které byly či jsou právě prováděny. V poslední kapitole je shrnuto, jaké doporučení je třeba k souladu ještě splnit.

Charakteristika e-mailových služeb VŠTE

E-mailové služby na VŠTE prochází stálým vývojem a přirozeným, dle aktuálních technických možností, trendů a potřeb organizace i koncových uživatelů, tak aby vždy byl zajištěn, pokud možno co nejoptimálnější stav. Charakteristiky prostředí jsou následující:

- Registrovány emailové 3 domény pod hlavní doménou vstecb.cz.
- Systém zahrnuje cca 5000 schránek, prozatím 2 distribuční list, do budoucna je připraveno další dělení do více distribučních listů, jak studentů podle oboru, tak zaměstnanců podle ústavu, ke kterému přísluší. Asociovány licence MS 365 A5. Veškeré objekty pro příjem (recipient objekty) v online cloudovém režimu (schránky, sdílené schránky, distribuční listy).
- Provozujeme plně hybridní prostředí Exchange Online s Exchange on premise servery pro management.
- Oficiální klient pro práci s poštou je MS Outlook 365, Outlooku on web, Outlook pro iOS a Android. Uživatelům je poskytována podpora pro registrované desktopy a zařízení v doméně nebo v M365.
- Emailové služby lze také používat přímo v prostředí studijního informačního systému IS.
- V oprávněných případech je povoleno používat systémy pro hromadné odesílání zpráv, např. pro oslovování uchazečů, hromadný kontakt studentů či zaměstnanců a PR akce.

Doporučení NPO realizovaná v e-mailových systémech VŠTE

V následujícím textu je shrnut soulad organizace s doporučeními řešitelské skupiny NPO-C2 PS2 (https://servicedesk- muni.atlassian.net/wiki/spaces/MS365SEC/pages/569606153/Zv+en+zabezpe+en+prost+ed+O365).

Řešitelé doporučení seskupili do následujících kategorií:

- Prevence
- Revize
- Monitoring, detekce
- Reakce

Stav souladu jednotlivých doporučení je rozepsán do kapitol, které odpovídají uvedeným kategoriím.

Prevence

Budování povědomí o rizicích a jejich cvičné vyšetřování

V rámci prevence se v prostředí VŠTE chystáme provést cvičnou phishingovou kampaň, jejíž účelem bude odhalit případná slabá místa v povědomí a uživatelského chování uživatelů, respektive zaměstnaneckých uživatelských účtů. Výsledný report z phishingového šetření pak bude prodiskutován a vyhodnocen tak, aby se fokusoval důraz na případné kritické chování v edukačním programu pro zaměstnance, jehož cílem je vzdělání zaměstnanců ohledně informačně bezpečnostního chování podobným principem, jako probíhá vzdělávání BOZP a PO. Pro zaměstnance se právě připravuje vzdělávací aktivita v LMS Moodle, jejíž velkou součástí je bezpečné chování při užívání pošty, volba a správa hesel a další chování v systémech v prostředí VŠTE.

Publikujte technické kontakty a nápovědu

- Veřejné (obecné) kontaktní informace organizace
  - podpora@vste.cz (sdílená schránka, přístup e-mail admins)
  - podpora@vste.cz (distribuční list s členy správců sítí, odboru bezpečnosti, e-mail admins atd.)
  - Security.txt – publikován na adrese https://www.vste.cz/.well-known/security.txt

```
Contact: podpora@vste.cz
Contact: https://www.vstecb.cz/kontakt-3-htm/
Preferred-Languages: en, cs
Canonical: https://www.vste.cz/.well-known/security.txt
```

- Technické kontakty
  - pro podporu ze strany Microsoft – nastaven kontakt na správce M365

- pro podporu koncových uživatelů - podpora@vste.cz
- Informace o ochraně dat pro koncové uživatele –nastaveny

- Technické kontakty uvnitř organizace – kontakty známé, komunikace prostřednictvím aplikace helpdesk
- Technické kontakty mimo organizaci – kontakty známé, ale nejsou publikované veřejně

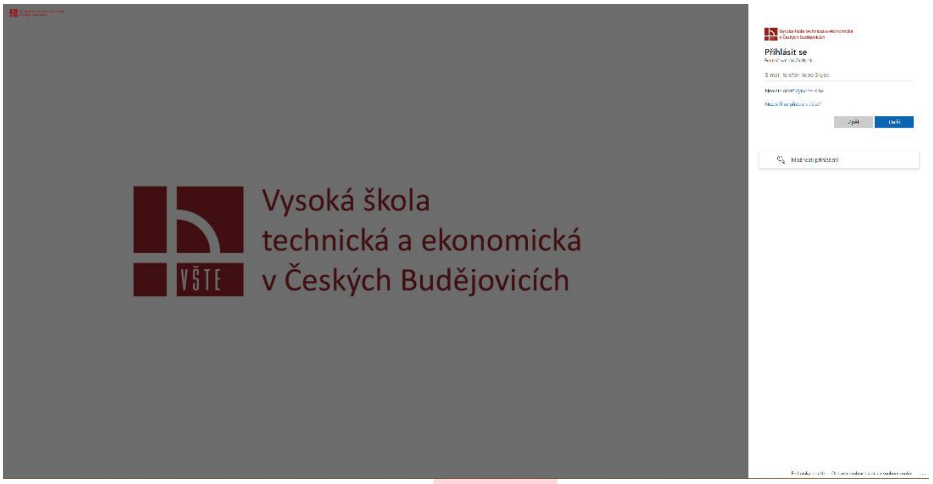
V prostředí VŠTE bylo zvažováno založení kontaktních e-mailových adres dle doporučení pracovní skupiny 2, ale nakonec bylo rozhodnuto s ohledem na velikost organizace využívat pouze jedinou emailovou adresu, kde se dále třídí požadavky dle jejich obsahu na příslušné pracovníky s příslušnou důležitostí. Tento systém je historicky v našich podmínkách ověřený a ze strany koncového uživatele je mnohem praktičtější s ohledem na potřebu si zapamatovat jediný kontakt, což může v kritickém bodě ušetřit čas i případné zmatky a nejistoty na straně uživatele, protože samotné třídění podnětů je následně v dikci odborníků.

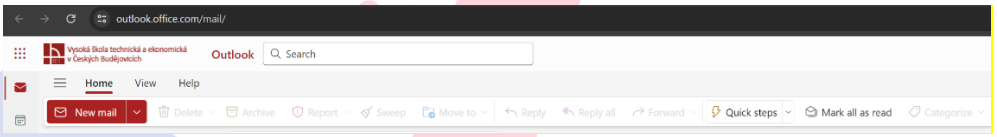
Používejte odkazy směřující na váš tenant a připravte zapamatovatelná přesměrování

- Nastaveno přesměrování URL

autodiscover.vste.cz	1800	CNAME	autodiscover.outlook.com	[Upravit | Smazat]
autodiscover.znalci.vste.cz	1800	CNAME	autodiscover.outlook.com	[Upravit | Smazat]
vste.cz	1800	MX	0 vste-cz.mail.protection.outlook.com	[Upravit | Smazat]
znalci.vste.cz	1800	MX	0 znalci-vste-cz.mail.protection.outlook.co...	[Upravit | Smazat]
vste.cz	1800	TXT	v=spf1 include:spf.protection.outlook.co...	[Upravit | Smazat]
znalci.vste.cz	1800	TXT	v=spf1 include:spf.protection.outlook.co...	[Upravit | Smazat]

Upravte branding přihlašování a prostředí MS 365





Zabezpečte Azure AD Connect

- Azure Aactive Directory Connect je nastaven a zabezpečen dle požadovaných specifikací.

Oddělte admin a uživatelské účty správců a nastavte přesměrování admin schránek

- Administrátorské a provozní účty jsou vzájemně oddělené.
- Administrátorské účty s emailovou schránkou mají nastaven provozní účet jako delegáta, kontrola pošty probíhá delegováním přístupu.
- Administrátorské účty podléhají pravidelné revizi. Odebírání přístupů probíhá manuálně na základě pravidelného auditu.
- Administrátorské účty jsou zabezpečeny více faktorovým.

Vytvořte záchranné účty globálních administrátorů

- Záchranný účet je již historicky vytvořen a nastaven, je přístupný pomocí systému „bílé obálky". Přístupové údaje k záchranným administrátorským účtům jsou uloženy v trezoru s více faktorovým fyzickým zabezpečením. Zároveň probíhá jeho pravidelná revize k ověření funkčnosti a dostupnosti, viz. kap. Revize

Nevytvářejte anonymní účty, účty se sdíleným heslem

- V prostředí VŠTE existuje pouze několik málo přesně definovaných účtů, které nejsou přiřazeny na konkrétní osobu, ale na předem známou skupinu dvou a více osob. Jedná se výhradně o odůvodněné případy a s přesně definovanými pravidly a osobami spojenými s danými účty.
- Jiné než specifikované a řádně odůvodněné neosobní účty nejsou povoleny.
- Servisní účty jsou vytvářeny jako neosobní, ale mají vždy vlastníka.

Nastavte omezení pro vytváření guestů a oprávnění guestů

- Tento typ účtů se v prostředí VŠTE nevyskytuje.

Nastavte synchronizaci hashí hesel

- Správa hesel je v prostředí VŠTE řešena výhradně pomocí studijního informačního systému IS, který se stará o správu hesel všech uživatelů do většiny systémů školy.

Zrušte expiraci uživatelských hesel

- Expirace hesel se v prostředí VŠTE nepoužívá.

Blokujte snadno prolomitelná hesla

- Politiky pro vytváření hesel je v prostředí VŠTE řízeno prostřednictvím studijního informačního systému IS, který se stará o správu a distribuci hesel do dalších systémů školy.

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

- Toto nastavení je již obsaženo v samotné nastavení Microsoftu, který je v prostředí VŠTE využíván.

Povolte/vynuťte vícefaktorové ověřování

- Nasazení MFA je v současné době v dlouhodobém strategické záměru IT oddělení a jeho nasazení se plánuje a připravuje.

Nastavte samoobslužný reset hesel

- Hesla se v prostředí VŠTE neresetují, dochází k distribuci hesel ze studijního informačního systému IS, tedy dojde-li ke změně hesla v ISu, heslo se změní i v dalších školních systémech.

Omezte/zakažte základní ověřování

- Nastaveno dle doporučení

Nastavte sledování a reakce na podezřelá přihlášení a ohrožené účty

- Ke sledování účtů v současné chvíli nedochází na úrovni školy, omezení významných účtů se řídí politikami nastavenými přímo ve studijním informačním systému IS.

Ověřte nastavení auditního logování

- Nastavení a využívání auditních logů je nyní ve fázi příprav a nasazení se plánuje.

Nastavte schvalování přístupu MS k datům tenantu

- Nepodporujeme, možné zprostředkování přes interní tiketovací a požadavkový systém, popřípadě kontaktováním pověřených pracovníku IT, vše v soulady s platnými pravidly školy.

Nastavte politiky pro ochranu pošty

- V současné chvíli se využívají pravidla pro ochranu pošty nastavená přímo ve studijním informačním systému IS, jehož součástí je pošta a dále na úrovni zabezpečení MS Office.
- Další způsoby zabezpečení a ochrany pošty jsou na IT oddělení diskutovány a připravovány k nasazení.
- V prostředí VŠTE je také kladen důraz na zabezpečení pošty již na úrovni myšlení uživatele, kdy je budováno povědomí o bezpečném nakládání a chování s poštovní schránkou.

Nasaďte doplněk pro hlášení (ne)vyžádané pošty

- Doplněk není plošně nasazen. Nastaven reporting na MS a zároveň sdílenou schránku.
- IT oddělení, kde dochází k vyhodnocení incidentu jak softwarově, tak na úrovni dohledu kompetentního odborníka z IT oddělení.
- Zároveň je hojně využíván automatický reporting v samotném systému MS 365, kde má VSŤE nastaveno mnoho bodů a pravidel k vyřešení nevyžádané pošty.

Nastavte upozorňování uživatelů na zprávy podezřelých odesílatelů

- Upozornění na první kontakt.
- Nastavení všech ostatních upozornění nastaveno dle doporučení.
- Průběžné budování bdělosti uživatele.

Nastavte upozorňování na spustitelné přílohy zpráv nebo je zablokujte

- Spustitelné přílohy jsou blokovány dle doporučení, včetně souborů s makry.

Omezte externí přesměrování zpráv

- Omezení externího přeposílání je zakázáno.

Omezte počet odeslaných zpráv za jednotku času

- Limit počtu příjemců jedné zprávy plošně nastaven defaultním nastavením MS Outlook.
- Vhodný limit počtu odeslaných zpráv se v prostředí VŠTE neřeší, stav je průběžně softwarově sledován a vyhodnocován, v případě potřeby je IT oddělení připraveno reagovat.

Autentizujte zprávy, zabraňte jejich podvržení, buduje reputaci svých domén

- Na všech doménách jsou nastaveny SPF záznamy, je aktivován DKIM (jak z Exchange Online, tak i z interního SMTP serveru).
- Stav autentizace odesílaných zpráv je pravidelně kontrolován. VŠTE je vlastníkem Premium licence, která umožňuje automatizovanou správu SPF a DMARC záznamů, správu subdomén a notifikace.
- DMARC autentizace odesílaných emailů za poslední 30 dnů dosahuje průměrné úspěšnosti převyšující 98% (údaj za poslední kalendářní rok).

Zpřesněte autentizaci odesilatelů při využití Gateway/Relay

- Všechny domény jsou směřovány MX záznamy přímo na Exchange Online, není třeba gateway řešit.

Ověřte, že máte povoleno auditování mailboxů

- Auditování mailboxů je povoleno.

Jak na autentizaci pošty

- Primární autentizační metody pošty – přehled splnění metod:
    - SPF – splněno pro všechny domény.
    - DKIM – splněno pro všechny domény.

Porovnejte aktuální nastavení s přednastavenými politikami dle Microsoftu

- Významná doporučení, především na uživatelské úrovni:
    - IT oddělení doporučuje využívat oficiální podpis do emailových služeb pro snazší identifikaci odesílatele
    - VŠTE klade důraz na budování povědomí a kritického myšlení uživatelů, tak aby koncový uživatelé byly v dostatečné informovanosti a připravenosti jak na případné incidenty, které se nepodaří zachytit softwarově, reagovat.

Omezte registraci a schvalování přístupu aplikací

- Registrace aplikací je v prostředí VŠTE zakázáno.

Zablokujte nepoužívané klientské protokoly

- Všechny klientské protokoly jsou monitorovány a v případě jejich nepoužívání po dobu stanovenou interním předpisem, jsou zablokovány.

Revize

Provádějte revize účtů se zvýšenými oprávněními

- Účty se zvýšenými oprávněními podléhají vyššímu nastavení sledování, viz kap. Revize
- Role v rámci Exchange Online
    - TenantAdmins_f00ce

Ověřujte dostupnost a funkčnost záchranných účtů

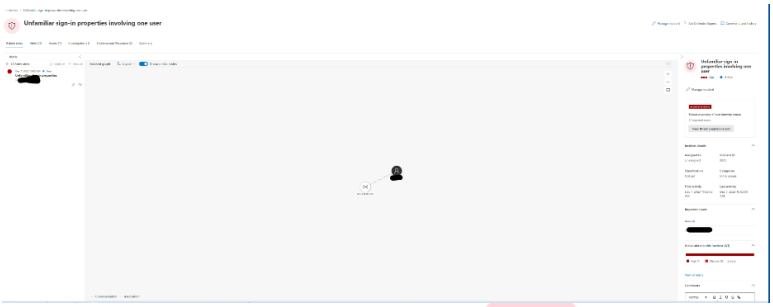
- Viz kap. Prevence

Aktualizujte systémy, komponenty a aplikace

- OS pravidelná aktualizace dle interních pravidel.
- Všechny aktualizace probíhají přímo z online prostředí, dle přesně definovaných pravidel.

Revidujte přehledy a inteligentní reporty

- Reporty s podrobným stavem aktuálního dění chodí v pravidelném týdenním intervalu pověřenému pracovníkovi na zabezpečený email.



Monitoring, detekce

Rizika/příznaky zneužití účtu (pro uživatele)

- Vytvořeny návody pro uživatele, tyto návody jsou přístupné ve variantě dostupné z prostředí Microsoft, dále pak existují návody ve studijním informačním systému IS.
- Samozřejmě jsou všichni pracovníci IT připraveni poskytnout konzultaci či odbornou asistenci.

Vyhodnocujte podezřelá přihlášení a ohrožené účty

- Detekce na riskantní přihlášení chodí globálním administrátorům a tyto případy jsou řešeny.
- Týdenní souhrny jsou odesílány na pověřené a definované pracovníky.

Nastavte a sledujte bezpečnostní upozornění

- Nastavení bezpečnostních upozornění je v souladu s doporučeními.
- Alerty jsou odesílány standardně na pověrné pracovníky.

Potvrďte ohrožení/zneužití účtu uživatele

Nastaven vnitřní proces pro kontrolu a revidování nahlášené (ne)vyžádané pošty

- Uživatelská hlášení podezřelých zpráv jsou možná těmito způsoby:
    - Odesláním vzorku podezřelé zprávy na spam@vste.cz.
    - Oznámením podezřelé zprávy jako SPAM/HAM přímo doplňkem Report Message v Outlooku.
    - Odesláním vzorku na oddělení bezpečnosti bezpecnost@vste.cz.
- Každé hlášení od uživatele je v co nejkratší době zpracováno a následně je uživateli odeslána zpráva s informací, zda je zpráva škodlivá či ne, jak s ní dále bylo či bude naloženo, respektive zda byla nahlášena na bezpečnostní portál Microsoftu k blokování.

Analýza falešně pozitivních/negativních detekcí spam/phish (draft)

- Uživatelská hlášení z doplňku Report Message jsou přeposílána na Microsoft ke zpracování a zároveň do schránky spam@vste.cz pro kontrolu administrátorem e-mailového systému.

Revidujte poštovní karanténu

- V prostředí VSŤE jsou veškeré abnormality a podezřelé chování monitorovány softwarovým řešením, na správný průběh monitoringu pak dohlížejí pověření kompetentní pracovníci, kteří s případnými abnormalitami dále operují k vyřešení daného problému, zároveň se touto cestou snažíme monitorovat trendy a dle toho aktivně reagovat v nastaveních pro boranu před případnými nežádoucími jevy.

Revidujte povolené/blokované odesilatele spoofovaných zpráv

- Kontrola odesílání za vlastní domény VŠTE je nastavena.
- Kontrola odesílání za cizí domény ve fázy implementace.

Reakce

Vyšetřování phishingových zpráv

- Detekce phishingových zpráv obvykle nastává po nahlášení podezřelé zprávy uživateli emailových služeb jedním ze způsobů v kapitole Monitoring a detekce.
- Nahlášenou podezřelou zprávu analyzuje e-mail software nebo některý z pověřených IT pracovníků (zpracovatel) a posílá uživateli zpět zprávu s výsledkem analýzy a provedené akci.
- Pokud je zpráva detekována jako phishing, vyhledává zpracovatel případné další zprávy s podobnou charakteristikou (podobné URL ve zprávě, podobný předmět, přílohy…) a nahlásí je na bezpečnostní portál Microsoftu. Pokud zpráva obsahuje škodlivé URL nahlásí je v Submissions a také na phishtank.com, google.com, eset.cz (ošetření případných přeposlaných zpráv). Případně blokuje URL na firewallu alespoň pro interní uživatele. Dále může být blokována adresa či odesílatel, pokud hrozí příjem dalších škodlivých.
- Pokud jde o phishing s vysokým nebezpečím (cílený obsah na organizaci, snaha simulovat standardní portály Microsoftu atp.) je provedena i okamžitá remediace přesunem škodlivých zpráv do složky SPAM. V opačném případě by měl zafungovat systém ZAP a přesunout zprávu automaticky po analýze Microsoftu.
- Samozřejmě je u každého incidentu provedeno šetření, zda někdo reagoval na zprávu – kontrola odpovědí v message trace a upozornění, aby již na škodlivé zprávy uživatelé neodpovídali. Dále je doporučeno kontrolovat URL prokliky.

- U uživatelů, kteří provedli nežádoucí akci, je provedeno příslušné vyšetřování – pokud je URL nahlášeno včas, Defender notifikuje prokliky na nebezpečné URL ze stanic registrovaných v Azure. Je-li podezření na únik hesla uživatele, je vyžádána změněna hesla uživatele (helpdesk).
- Po ukončení analýz je provedena kontrola, zda remediace zpráv proběhla požadovaným způsobem a u všech zpráv (Explorer).
- U případných odpovědí na incidentní zprávu je pak zhodnoceno, zda bylo možné u daného uživatele předejít reakci na email lepším proškolením zaměstnance, či zvýšení povědomí o možnostech, jak podezřelé zprávy identifikovat.

Remediace úniku/zneužití přihlašovacích údajů uživatele

- Je-li podezření na únik přihlašovacích údajů (Identity Protection / Risky User či reakce na phishing), je účet buď automaticky zablokován nebo je zablokován adminem. Je vhodné revokovat aktivní spojení a zakázat klientské protokoly ke schránce (MAPI, ActiveSync, EWS, Outlook on the web).
- Je provedena analýza útoku (Azure AD / Security / Sign-Ins) a pokud je potvrzeno zneužití, je ošetřeno zařízení, ze kterého přihlášení nastalo (antivirová kontrola, updaty OS..).
- Po kontrole akcí auditem a opravě všech podezřelých změn je účet reaktivován a je vyžádána změna hesla uživatele.

Nouzové povolení cloudového přihlášení v případě výpadku pass-through nebo federovaného přihlášení

- Přihlášení je funkční I při výpadku Azure Active Directory Connect serveru.

Správa výjimek (povolování/blokování) při filtrování pošty

- Nahlášení zprávy
  - je použito vždy, pokud je zpracování ze strany MS Defenderu chybné.
- Nastavení výjimky
  - Je použito v případě, že Defender po nahlášení zprávy nadále detekuje s chybou.
  - Řešení falešných detekcí impersonation
    - Nastaveny výjimky typu doména (vste.cz, respektive vstecb.cz vs. vse.cz – obě korektní a často zaměňované).
  - Tenant Allow/block lists
    - Výjimky na povolení/blokování adres a domén, historicky nebo na základě hlášení phishingů nebo korektních zpráv blokovaných jako SPAM. Bývá použita expirace platnosti výjimky (zejm. v případě povolení).
  - Transportní pravidla EXO

        - Použito pro SPAMy a Phishingy opakovaně detekované jako korektní e-maily (např. Phishingy typu „Výzva daňového úřadu“). Využito schvalování doručení.
    - Uživatelský seznam blokovaných odesílatelů a domén v Outlooku
        - Jeho správa je ponechána na uživateli.
        - Je uživatelům doporučováno použít, pokud se jedná o individuální SPAMy.
    - IP Allow/Block lists + Safe list v Connection filter policy
        - Povolení dalších SMTP serverů pro nastavení mailflow
        - Zakázání SMTP serverů, kterých bylo v minulosti detekováno rozesílání SPAM
    - Povolení pro simulace phishingových kampaní
        - Výjimky pro systém simulující tréninkové phishingové kampaně. Nepoužito, ošetřeno transportním pravidlem.

Zablokujte nebezpečnou URL adresu nebo soubor

- Viz kapitola Reakce

Smažte (nebezpečnou) doručenou zprávu

- Použito běžně pro ošetření doručených nebezpečných zpráv. Není využito odstranění zpráv, ale přesun do složky SPAM, dle platných nastavených pravidel pro nakládání se zprávou tohoto typu.

Opravte nastavení schránky

- Součástí remediace po zneužití e-mailové schránky.

Odeberte uživatele ze seznamu blokovaných odesílatelů

- Informace o blokovaném odesílání přichází e-mail pověřeným pracovníkům, respektive v prostředí VŠTE IT týmu.

Odblokujte tenant po vlně odchozího spamu

- Je nastavena notifikace na příslušné kompetentní pracovníky IT oddělení e-mailu, že bylo provedeno a zaznamenáno blokování odesílání.

Nahlaste zprávu Microsoftu na přezkoumání

- Hlášení zpráv je běžně používáno, jak ze strany IT pracovníků, tak ze strany uživatelů, díky budování povědomí o možných rizikových situacích a chování v nich.

Doporučení, která je třeba ještě splnit

Systém Microsoft 365 se neustále dynamicky vyvíjí a zejména v oblasti zabezpečení e-mailu došlo v posledních dvou letech ke značnému pokroku. Zejména bylo třeba stanovit a prakticky nasadit procesy zpracování bezpečnostních incidentů, zmapovat toky e-mailové komunikace a zlepšit její autentizaci a bezpečnost. Nadále zůstává několik důležitých aspektů nedořešeno a bude třeba na jejich uvedení do provozu pracovat.

Boj s potencionálními útočníky a s pokusy o rozesílání spamu, podvodných emailů a další je věc, které se nedá vyřešit jednorázově, ale jedná se o záležitost kontinuální a dlouhodobou, v prostředí VŠTE se tedy snažíme sledovat stav, monitorovat situaci a se všemi případnými incidenty držet krok. Provádíme tady pravidelné revize, sledujeme reporty, budujeme situační povědomí na straně uživatelů, s kterými se snažíme být maximální možnou mírou v kontaktu, analyzujeme stavy v síti, chování uživatelů i jednotlivé incidenty, ať už reálně pozitivní či falešně pozitivní a hledáme rezervy a další možnosti ve zlepšení nastavení zabezpečení.

Výstup číslo 5, NPO nám poskytl možnost jisté míry reflexe, kdy jsme ve velké části doporučení měli již realizovány či jsme svým zabezpečením dokonce převýšili, další velkou část doporučení jsme díky tomuto projektu realizovali dříve nebo lépe než byl původní strategický plán a zbylá malá část doporučení je prozatím ve strategickém plánu a jejich nasazení či realizace se chystá či zvažuje.