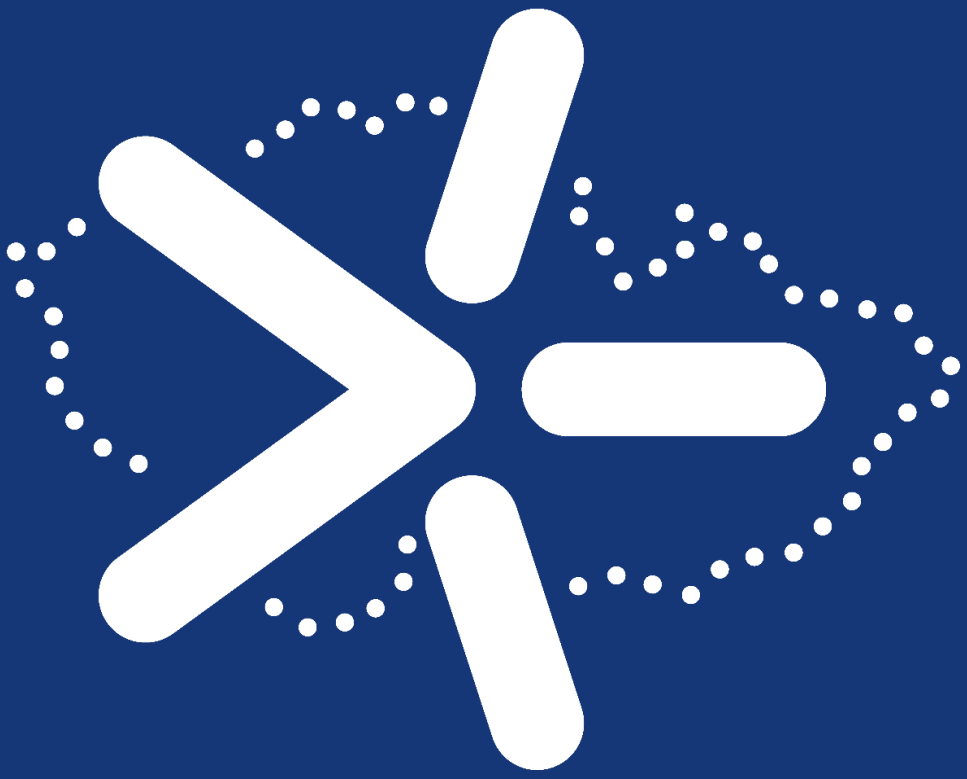

VÝSTUP Č. 1 ČZU

Posouzení a případná realizace zabezpečení kolaborativní platformy, včetně jejího pokročilého nastavení.

Cíl: Analýza a výběr vhodných komponent kolaborativní platformy, včetně identifikace a posouzení stavu implementace již užívaných řešení pro potřeby zajištění distančního vzdělávání dle již existujících doporučení, standardů či metodik.

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

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

Obsah

Zabezpečení emailových služeb ČZU

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 České zemědělské univerzitě v Praze (ČZU) byly v průběhu projektu NPO provedeny změny v nastavení zabezpečení e-mailu odpovídající těmto doporučením. Jejich přehled je předmětem tohoto dokumentu. Je třeba upozornit, že ke změnám dochází průběžně a tento dokument zachycuje stav ke konci června 2023.

V první kapitole je v hrubých rysech přiblížena topologie e-mailových služeb provozovaných na ČZU, s důrazem na technologie podporované oddělením OIKT (Odbor informačních a komunikačních technologií). V následujících kapitolách je bodově shrnuto, která doporučení univerzita splňuje a na kterých se případně pracuje. V poslední kapitole je shrnuto, jaké doporučení je třeba k souladu ještě splnit.

Charakteristika e-mailových služeb ČZU

E-mailové služby na ČZU prošly od roku 2003 vývojem od separátních SMTP serverů na jednotlivých fakultách přes centralizované on-premise systémy (GroupWise a později on-premise Exchange servery) až k současnému hybridnímu modelu Exchange online. Charakteristiky prostředí jsou následující:

- Registrováno 30 domén pod hlavní doménou czu.cz.
- Systém zahrnuje cca 40000 schránek, cca 800 distribučních listů. 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.
- V oprávněných případech je povoleno používat externí systémy pro hromadné odesílání zpráv, např. MailChimp, MlSend atp, např. pro oslovování uchazečů a PR akce.

Doporučení NPO realizovaná v e-mailových systémech ČZU

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

Publikujte technické kontakty a nápovědu

- Veřejné (obecné) kontaktní informace organizace
  - postmaster@czu.cz (sdílená schránka, přístup e-mail admins)
  - abuse@czu.cz (distribuční list s členy správců sítí, odboru bezpečnosti, e-mail admins atd.)
  - Security.txt – publikován na adrese czu.cz/.well-known/security.txt
- Technické kontakty
  - pro podporu ze strany Microsoft – nastaven kontakt na správce M365
  - pro podporu koncových uživatelů - helpdesk@czu.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

Upravte branding přihlašování

- Branding nakonfigurován, přidáno logo ČZU

Používejte odkazy směřující na váš tenant a připravte zapamatovatelná přesměrování

- Nastaveno přesměrování URL https://mail.czu.cz na https://outlook.office365.com/czu.cz

Upravte branding prostředí MS 365

- Branding nakonfigurován, přidáno logo ČZU

Zabezpečte Azure AD Connect

[Sem zadejte text.]

- AADC dle specifikovaných požadavků zajištěn.

Oddělte admin a uživatelské účty správců a nastavte přesměrování admin schránek

- Administrátorské účty jsou oddělené od provozních.
- Administrátorské účty s emailovou schránkou mají nastaven provozní účet jako delegáta, kontrola pošty probíhá delegováním přístupu.
- Provádí se pravidelná revize administrátorských účtů. Odebírání přístupů probíhá manuálně na základě pravidelného auditu.
- Striktně je pro administrátorské účty požadováno více faktorové ověřování.

Vytvořte záchranné účty globálních administrátorů

- Záchranný účet nastaven, přístupný pomocí systému „bílých obálek".

Nevytvářejte anonymní účty, účty se sdíleným heslem

- Snaha je neosobní účty nevytvářet a požadavky na ně potlačovat a preferovat sdílené schránky. Přesto jich několik existuje (např. pro odesílání notifikací). Některé aplikace nepodporují jiný způsob autentizace než heslem. Každý neosobní účet má definovaný osobní účet jako vlastníka (atribut manager).
- Servisní účty jsou vytvářeny jako neosobní, ale mají vždy vlastníka.

Nastavte omezení pro vytváření guestů a oprávnění guestů

- Omezení pro vytváření a oprávnění Guest účtů jsou nastavena v souladu s doporučeními

Nastavte synchronizaci hashí hesel

- Synchronizace je nastavena v souladu s doporučeními.
- *Je nastavena kontrola uniklých hesel v Azure AD Identity Protection.*

Zrušte expiraci uživatelských hesel

- Nastaveno v souladu s doporučeními.

Blokujte snadno prolomitelná hesla

- Global banned password list – nastaven režim „Audit".
- Custom banned password list – nejsou nastaveny blokované termíny.

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

- Nastavení není nutné provádět, je provedeno ze strany Microsoftu.

Povolte/vynuťte vícefaktorové ověřování

- Nasazení MFA dle doporučení je splněno částečně, v současnosti probíhá pro zbývající provozní části ČZU.

Nastavte samoobslužný reset hesel

Nastaveno dle doporučení

[Sem zadejte text.]

Omezte/zakažte základní ověřování

-
- Nastaveno dle doporučení

Nastavte sledování a reakce na podezřelá přihlášení a ohrožené účty

Sledování privilegovaných účtů nastaveno

Ověřte nastavení auditního logování

Auditní logy zapnutyZajistěte dostupnost historie doručených/odeslaných zpráv

Dostupnost zajištěna až po dobu 90 dní.

Nastavte schvalování přístupu MS k datům tenantu

-
- Nepodporujeme, možné zprostředkování přes interní tiketovací systém.

Nastavte politiky pro ochranu pošty

- Politiky pro karanténu
  - Upravena doba uchování karantény na 30 dnů.
  - Uživatelům v standardních politikách nastavena notifikace na výskyt e-mailu v karanténě. Povoleno uvolnění e-mailu nebo poslání žádosti o uvolnění v případě vysoce hodnocených spamů a malware.
  -
- Nastaveny politiky pro ochranu proti malware, spamu, phishingu (inbound)
- Nastavena Safe links policy
- Nastavena Safe Attachments policy
- Nastavena Safe Documents policy

Nasaďte doplněk pro hlášení (ne)vyžádané pošty

- Doplněk není plošně nasazen. Nastaven reporting na MS a zároveň sdílenou schránku spam@oikt.czu.cz .

Nastavte upozorňování uživatelů na zprávy podezřelých odesílatelů

- Upozornění na první kontakt
- Nastavení všech ostatních upozornění nastaveno dle doporučení.

Nastavte upozorňování na spustitelné přílohy zpráv nebo je zablokujte

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

Omezte externí přesměrování zpráv

Přesměrování a přeposílání pošty je v současnosti povoleno, bude zakázáno po vydání aktualizované směrnice pro oblast emailové komunikace.

Omezte počet odeslaných zpráv za jednotku času

[Sem zadejte text.]

- Limit počtu příjemců jedné zprávy plošně nastaven ve všech plánech na max. 500 příjemců.
- Vhodný limit počtu odeslaných zpráv za den/uživatele je momentálně předmětem interního šetření

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).
- Na všech doménách je aktivována DMARC politika „quarantine" a je nastaveno zasílání DMARC reportů.
- Stav autentizace odesílaných zpráv je pravidelně kontrolován nástrojem https://valimail.com , který je doporučovaný pro M365 Microsoftem a je dostatečný pro automatizované zpracování XML DMARC reportů. Uvažujeme o pořízení Premium licence, která umožňuje automatizovanou správu SPF a DMARC záznamů, správu subdomén a notifikace.
- DMARC autentizace odesílaných emailů za poslední 30 dnů dosahuje úspěšnosti 99,39% (k 12.7.2023).

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.
  - DMARC - splněno pro všechny domény.
  - DMARC ARC – nepoužíváme, není zatím větší problém s přeposíláním.
  - DNSSec – nesplněno – postupná implementace řešení .

Porovnejte aktuální nastavení s přednastavenými politikami dle Microsoftu

- Významná doporučení:
  - Omezit Allowed Senders a Allowed Sender Domains

Omezte registraci a schvalování přístupu aplikací

- Registrace aplikací nyní není omezená. Doporučeno je omezit registraci aplikací jen na oprávněné uživatele.

Zablokujte nepoužívané klientské protokoly

- Protokol POP3 není povolen
- Protokol IMAP omezen.
- Autentizovaný protokol SMTP k serveru smtp.office365.com maximálně.

Revize

Provádějte revize účtů se zvýšenými oprávněními

- Viz. Prevence / „Nastavte sledování a reakce na podezřelá přihlášení a ohrožené účty".
- Aktuální výpis rolí (Get-MsolRole | Sort-Object -Property Name | ForEach-Object { $role = $_; Get-MsolRoleMember -RoleObjectId $_.objectid | ForEach-Object { $role.name + ": " + $_.displayname } }):
- Role v rámci Exchange Online
  - Application Impersonation
  - GlobalReaders_-2049125727
  - Organization Management
  - Recipient Management
  - SecurityReaders_-1529400320
  - TenantAdmins_f00ce
  - View-Only Organization Management

Ověřujte dostupnost a funkčnost záchranných účtů

- Viz. Prevence / „Vytvořte záchranné účty globálních administrátorů".
-

Aktualizujte systémy, komponenty a aplikace

- OS pravidelná aktualizace dle interních pravidel. Security updaty ihned.
- Minimalizace Exchange On Premise udržujeme s posledními Security Updaty.

[Sem zadejte text.]

- Compliance management – doporučené nastavení

Revidujte přehledy a inteligentní reporty

- Reporty dostupné. Nutno určit odpovědnosti.
- Přehledy a reporty z aplikace Exchange Insight a Reports

Monitoring, detekce

Rizika/příznaky zneužití účtu (pro uživatele)

- Vytvořeny návody pro uživatele.

Vyhodnocujte podezřelá přihlášení a ohrožené účty

- Detekce na riskantní přihlášení chodí globálním administrátorům a tyto případy jsou řešeny.
- Týdenní souhrny jsou odesílány na globální administrátory.

Nastavte a sledujte bezpečnostní upozornění

- Nastavení bezpečnostních upozornění je v souladu s doporučeními.
- Alerty jsou odesílány standardně na globální správce, některé jsou upravené tak, aby se odesílaly i na další příjemce.

Potvrďte ohrožení/zneužití účtu uživatele

Nastaven vnitřní proces pro kontrolu.Revidujte nahlášenou (ne)vyžádanou poštu

- Uživatelská hlášení podezřelých zpráv jsou možná těmito způsoby:
  - Odesláním vzorku podezřelé zprávy na spam@oikt.czu.cz.
  - Oznámením podezřelé zprávy jako SPAM/HAM přímo doplňkem Report Message v Outlooku.
  - Zadáním požadavku „Nahlášení podezřelé zprávy (SPAM, Phishing, SCAM...)“ v systému helpdesk.czu.cz.
  - Odesláním vzorku na oddělení bezpečnosti bezpecnost@czu.cz.
- Uživatelská hlášení jsou pravidelně zpracovávána a uživateli je odeslána informace, zda je zpráva škodlivá či ne a 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@oikt.czu.cz pro kontrolu administrátorem e-mailového systému.

Revidujte poštovní karanténu

- Uživatelům je odesílán pravidelně denní report o zachycených zprávách v karanténě.
- Uživatelé si mohou u nízko hodnocených zpráv provést uvolnění zprávy z karantény sami.
- Administrátor pravidelně kontroluje uvolněné zprávy v Review, pokud se jedná o chybně detekovanou korektní zprávu, předává vzorek k analýze na bezpečnostní portál Microsoftu.

[Sem zadejte text.]

- Vysoce hodnocené SPAMy a Phishingy nemůže uživatel sám uvolnit, nutná kooperace s adminem.

Revidujte povolené/blokované odesilatele spoofovaných zpráv

- Kontrola odesílání za vlastní domény ČZU 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 „Revidujte nahlášenou (ne)vyžádanou poštu".
- Nahlášenou podezřelou zprávu analyzuje e-mail admin nebo bezpečnostní technik (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.
- Je doporučena kontrola, zda někdo na zprávu reagoval – 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, proveďte 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).

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

[Sem zadejte text.]

- Přihlášení je funkční I při výpadku AAD 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 (zcu.cz vs. czu.cz – obě korektní a často zaměňované).
  - Tenant Allow/block lists
    - Výjimky na povolení/blokování adres a domén, obvykle 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 „Předvolání Policie ČR"). Využito schvalování doručení.
    - Ošetření e-mailů označených z jiných systémů jako SPAM – nastavení vyšší Spam Confidence Level.
  - 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 – např. smtps.czu.cz .
    - Zakázání SMTP serverů, které v minulosti rozesílali SPAM
  - Allowed senders/domains, Blocked senders/domains v antispam politikách
    - Není již doporučeno používat a mělo by být nahrazeno výjimkami v „Tenant Allow/block lists".
  - Povolení doručování pro SecOps mailboxy
    - Schránky bez jakýchkoli kontrol – spam@oikt.czu.cz a postmasterCZU@czu.cz .
  - Povolení pro simulace phish kampaní
    - Výjimky pro systém simulující tréninkové phishingové kampaně. Nepoužito, ošetřeno transportním pravidlem.

Zablokujte nebezpečnou URL adresu nebo soubor

- Viz. „Vyšetřování phishingových zpráv".

Smažte (nebezpečnou) doručenou zprávu

- Použito běžně pro ošetření doručených nebezpečných zpráv. Není využito odstranění zpráv, ale přesun do složky SPAM.

Opravte nastavení schránky

- Součástí remediace po zneužití e-mailové schránky.

[Sem zadejte text.]

Odeberte uživatele ze seznamu blokovaných odesílatelů

- Informace o blokovaném odesílání přichází e-mail administrátorům.

Odblokujte tenant po vlně odchozího spamu

- Je nastavena notifikace na administrátory e-mailu a globální administrátory, že k blokování odesílání došlo.

Nahlaste zprávu Microsoftu na přezkoumání

- Hlášení zpráv je běžně používáno, i ze strany znalých uživatelů.

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. Jedná se zejména o tato doporučení v souladu s projektem NPO:

- Nasazení zabezpečení DNSSec na DNS serverech ČZU – je též požadováno pro organizace s vyhrazenou infrastrukturou a spadající pod regulaci dle vyhlášky NÚKIB 82/2018 Sb.
- Omezení forwardu z e-mailových schránek – bohužel běžná (a špatná) praxe všech uživatelů e-mailu. Přesto bude vhodné z důvodu bezpečnosti a úniku informací přeposílání v maximální míře omezit. Bude provedeno po vydání nové směrnice pro oblast bezpečnosti ICT, která přeposílání mimo organizace zakáže.
- Nasazení MFA pro všechny uživatele ČZU – probíhá postupně po jednotlivých součástech ČZU, opatření naráží na odpor z důvodu např. údajně menšího „komfortu“ práce.
- Omezení registrace aplikací Azure AD kýmkoli – vhodnější model by byl umožnit registraci jen osobám oprávněným aplikace a koncová zařízení spravovat, nebo alespoň nasadit schvalovací workflow. Tato problematika je nad rámec správy emailových systémů, přestože se i e-mailových aplikací (klientů) týká.
- Dořešení a optimalizace antispamových a antiphishingových politik. Tyto úpravy jsou v procesu postupného zlepšování.
- Další změny nastavení:
    - Optimalizované limity pro odesílání z mailboxu za hodinu, za den, dle prostředí
- Vylepšit automatické stahování SMTP logů (skripty MUNI).
- Vylepšit proces zpracování podezřelých zpráv – kontrola reakcí uživatele, ošetřovat též následky úniku přihlašovacích údajů (okamžitá revokace spojení a Purview audit) a informovat na přeposlané zprávy.
- Určit pravidelné kontroly reportů, revize politik, seznamu globálních správců. Určit správce a zodpovědnost za jednotlivé funkční celky.

[Sem zadejte text.]