Ministerstvo vnitra České republiky

Žádost o poskytnutí informací podle zákona č. 106/1999 Sb.

Dne [redacted] v 16:55:37 UTC se server služby Informace pro všechny / mySociety pokusil doručit mou žádost podle zákona č. 106/1999 Sb. na elektronickou adresu [redacted]

S[redacted] M[redacted] vnitra smtp-mvcr.gov.cz zprávu odmítl s následující diagnostikou:

550-#5.7.1 Your access from IP [redacted] to this e-mail system has been rejected due to poor reputation on Talosintelligence.com

550 or DNS Lookups, where Forward and Reverse DNS lookups do not Match.

Zpráva tedy nebyla elektronickou podatelnou přijata.

Ministerstvo vnitra současně veřejně uvádí elektronickou adresu posta@mv.gov.cz jako elektronickou adresu své podatelny a uvádí, že datovou zprávu lze doručit zasláním e-mailové zprávy na tuto adresu.

V této souvislosti žádám podle zákona č. 106/1999 Sb. o následující informace:

1. Konkrétní důvod odmítnutí zprávy

Uveďte konkrétní technický důvod, pro který byla dne [redacted] v 16:55:37 UTC odmítnuta zpráva přicházející z IP adresy [redacted]

Uveďte zejména, zda důvodem bylo:

a) hodnocení reputace IP adresy službou Cisco Talos / Talos Intelligence,
b) nesoulad forward a reverse DNS záznamů,
c) oba uvedené důvody,
d) jiný důvod.

2. Záznam o konkrétním odmítnutí

Poskytněte existující log, výpis, záznam nebo jiný dokument zachycující uvedené odmítnutí zprávy, v rozsahu, v jakém jej lze poskytnout bez zveřejnění bezpečnostně citlivých technických informací.

Pokud byl původní e-mail nebo jeho metadata nějakým způsobem uchovány i přes jeho odmítnutí, uveďte tuto skutečnost.

3. Pravidla pro automatické odmítání zpráv

Poskytněte aktuální vnitřní předpis, metodiku, provozní pravidlo, bezpečnostní politiku nebo jiný dokument, který upravuje automatické odmítání příchozích e-mailových zpráv směřujících na elektronickou podatelnu Ministerstva vnitra na základě:

reputace IP adresy odesílajícího serveru,
blacklistů či reputačních databází,
kontroly DNS,
kontroly forward/reverse DNS,
jiných obdobných reputačních nebo technických kritérií.

Pokud takový dokument neexistuje, žádám o výslovné sdělení této skutečnosti.

4. Využívané externí reputační služby

Uveďte, zda Ministerstvo vnitra při rozhodování o přijetí nebo odmítnutí zprávy na elektronické podatelně využívá službu Cisco Talos Intelligence.

Uveďte rovněž názvy dalších externích blacklistů, reputačních databází nebo obdobných služeb, jejichž výsledek může automaticky vést k odmítnutí příchozí zprávy.

Nežádám o konkrétní bezpečnostní konfiguraci, autentizační údaje ani jiné údaje umožňující ochranný systém obejít.

5. Právní a organizační podklad

Uveďte, který útvar Ministerstva vnitra rozhodl o zavedení uvedeného mechanismu a kdo je odpovědný za jeho provoz a nastavení.

Poskytněte existující dokument zachycující schválení či odůvodnění tohoto způsobu ochrany elektronické podatelny.

6. Vztah ke zveřejněným podmínkám elektronické podatelny

Uveďte, na základě kterého konkrétního zveřejněného pravidla nebo podmínky přijímání dokumentů elektronickou podatelnou Ministerstva vnitra byla zpráva z IP adresy [redacted]

Pokud Ministerstvo vnitra nemá mezi veřejně zveřejněnými podmínkami přijímání dokumentů uvedeno, že zpráva může být odmítnuta z důvodu reputace odesílající IP adresy, externího blacklistu nebo nesouladu forward/reverse DNS, žádám o výslovné sdělení této skutečnosti.

7. Kontrola falešně pozitivních výsledků

Uveďte, jaký mechanismus Ministerstvo vnitra používá pro zjišťování a nápravu případů, kdy je legitimní zpráva elektronické podatelně automaticky odmí
tnuta jako důsledek reputačního nebo antispamového pravidla.

Uveďte zejména:

zda jsou odmítnuté zprávy nebo jejich metadata následně kontrolovány pracovníkem ministerstva,
zda existuje postup pro dodatečné povolení legitimního odesílajícího serveru,
kdo o takovém povolení rozhoduje,
zda je možné zpětně zjistit, že automaticky odmítnutá zpráva byla úředním podáním.

8. IP adresa [redacted]

Uveďte:

zda je IP adresa [redacted] ke dni vyřízení této žádosti stále automaticky odmítána,
od kdy byla podle dostupných záznamů odmítána,
zda byla někdy na seznamu povolených adres nebo z blokování vyjmuta,
zda Ministerstvo vnitra eviduje, že jde o server infrastruktury mySociety, který je používán mimo jiné službami pro podávání žádostí o informace veřej
ným institucím.

9. Rozsah odmítání zpráv

Pokud Ministerstvo vnitra disponuje existujícími statistikami nebo jinými souhrnnými údaji, uveďte za roky 2025 a 2026:

počet příchozích e-mailových zpráv adresovaných elektronické podatelně, které byly odmítnuty již na úrovni SMTP,
z toho počet odmítnutí na základě reputace IP adresy nebo externí reputační databáze,
z toho počet odmítnutí z důvodu kontroly DNS nebo nesouladu forward/reverse DNS.

Pokud ministerstvo takové statistiky nevede a jejich vytvoření by vyžadovalo vytvoření nové informace, postačí výslovné sdělení této skutečnosti.

10. Známé případy legitimních podání

Uveďte, zda Ministerstvo vnitra v letech 2025 L 2026 zaznamenalo případy, kdy byla antispamovým či reputačním systémem odmítnuta zpráva, o níž se následně zjistilo, že obsahovala žádost podle zákona č. 106/1999 Sb. nebo jiné podání vůči orgánu veřejné moci.

Pokud ano a ministerstvo takovou evidencí disponuje, žádám o počet takových případů a obecné označení způsobu, jakým byly řešeny.

11. Změny pravidel

Poskytněte existující dokumenty zachycující změny pravidel automatického odmítání zpráv elektronickou podatelnou provedené od [redacted] pokud se týk
aly reputačních databází, blacklistů nebo kontroly DNS.

Nežádám o poskytnutí hesel, privátních klíčů, konkrétních bezpečnostních prahových hodnot, úplné konfigurace bezpečnostních zařízení ani jiných techni
ckých údajů, jejichž zveřejnění by reálně umožnilo obejít bezpečnostní opatření Ministerstva vnitra.

Pokud některá část požadovaného dokumentu takové chráněné informace obsahuje, žádám o poskytnutí zbývající oddělitelné části dokumentu.

Pokud některý požadovaný dokument nebo údaj neexistuje nebo jím Ministerstvo vnitra nedisponuje, žádám o výslovné uvedení této skutečnosti u příslušné
ho bodu.

M[redacted] Š[redacted]

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.

Typ vstupního dokumentu: .TXT
Otisk vstupního souboru: [illegible]
Použitý algoritmus: SHA256_SBB [illegible]

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, [illegible] Praha 7

Datum vyhotovení ověřovací doložky:
[illegible]

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
[illegible]

Elektronická pečeť - 28.8.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Ministerstvo
vnitra

MVCRX09EXLMS
prvotní identifikátor

odbor podpory IT
náměstí Hrdinů 1634/3
140 21 Praha 4

M Š
Vi P C
ID schránky:

Č. j. MV-139536-4/OPIT-2026
Vyřizuje R M
Telefon
E-mail radomir. gov.cz
Místo, datum Praha 18. září 2026
Počet příloh 2

Žádost o informace – odmítnutí e-mailu elektronickou podatelnou MV - odpověď
K č. j. MV-139536/AS-2026

Vážený pane Škope,

Ministerstvo vnitra České republiky obdrželo dne 28. srpna 2026 Vaši žádost o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, týkající se odmítnutí elektronické zprávy doručované na elektronickou podatelnu Ministerstva vnitra.

Povinný subjekt Vaši žádost posoudil a v souladu s § 14 odst. 5 písm. d) zákona č. 106/1999 Sb. poskytuje požadované informace.

Odpovědi na jednotlivé body žádosti jsou uvedeny v příloze č. 1 tohoto přípisu.

S pozdravem

Mgr. Kateřina Peterkova
ředitelka

1. <u>Konkrétní důvod odmítnutí zprávy</u>

Otázka:

Uveďte konkrétní technický důvod, pro který byla dne [redacted] v [redacted] UTC odmítnuta zpráva přicházející z IP adresy [redacted]. Uveďte zejména, zda důvodem bylo:

a) hodnocení reputace IP adresy službou Cisco Talos Intelligence,

b) nesoulad forward a reverse DNS záznamů,

c) oba uvedené důvody,

d) jiný důvod.

Odpověď:

Z dostupných provozních záznamů vyplývá, že při pokusu o doručení elektronické zprávy z IP adresy [redacted] dne [redacted] UTC došlo k odmítnutí SMTP spojení z důvodu neúspěšné kontroly DNS (DNS Validation Failed).

Povinný subjekt disponuje informací o neúspěšném výsledku DNS kontroly, nikoliv o odmítnutí z důvodu reputačního hodnocení IP adresy.

Na položenou otázku tedy povinný subjekt odpovídá, že podle dostupných provozních záznamů byl důvodem odmítnutí:

b) nesoulad forward a reverse DNS záznamů (DNS Validation Failed).

---

2. <u>Záznam o konkrétním odmítnutí</u>

Otázka:

Poskytněte existující log, výpis, záznam nebo jiný dokument zachycující uvedené odmítnutí zprávy.

Odpověď:

Ministerstvo vnitra poskytuje informace z dostupného provozního záznamu zachycujícího pokus o doručení zprávy dne [redacted]

- *čas pokusu o doručení: [redacted] **v [redacted]38 CEST**,*
- *zdrojová IP adresa: [redacted]*
- *odesílající server: [redacted]*
- *adresa odesílatele: [redacted]**cz**,*

- *adresa* [redacted]
- *výsledek kontroly reverzního DNS:* ***ověření neúspěšné****,*
- *výsledek zpracování:* ***SMTP spojení odmítnuto****.*

K odmítnutí došlo před přijetím a dalším zpracováním zprávy. Obsah zprávy nebyl Ministerstvem vnitra přijat ani uložen. Uchován byl pouze provozní záznam o pokusu o doručení.

V rozsahu identifikace interní síťové infrastruktury Ministerstvo vnitra informaci neposkytuje podle § 15 odst. 1 zákona č. 106/1999 Sb. ve spojení s § 11 odst. 1 písm. d) tohoto zákona.

---

3. <u>Pravidla pro automatické odmítání zpráv</u>

Otázka:

Poskytněte aktuální vnitřní předpis, metodiku, provozní pravidlo, bezpečnostní politiku nebo jiný dokument upravující automatické odmítání příchozích e-mailových zpráv.

Odpověď:

Povinnému subjektu nebyl dohledán samostatný vnitřní předpis ani metodika upravující provádění kontrol příchozího SMTP provozu, na které se dotaz vztahuje.

Technické parametry služby jsou popsány v katalogovém listu služby CMS [redacted] *„Příchozí SMTP provoz“. Tento katalogový list mimo jiné obsahuje volitelný parametr kontroly forward DNS a reverse DNS záznamů.*

Rozhodování o důvěryhodnosti (reputaci) zdrojů elektronické pošty není upraveno samostatným dokumentem povinného subjektu. Toto rozhodování je realizováno prostřednictvím interních mechanismů bezpečnostního produktu Cisco.

Povinnému subjektu nebyla dohledána samostatná metodika, interní předpis ani jiný dokument, který by obsahoval algoritmy, pravidla nebo kritéria používaná produktem Cisco pro reputační hodnocení zdrojů elektronické pošty, neboť se jedná o součást technologie vyvinuté a dodávané výrobcem tohoto produktu.

---

4. Využívané externí reputační služby

Otázka:

Uveďte, zda Ministerstvo vnitra při rozhodování o přijetí nebo odmítnutí zprávy využívá službu Cisco Talos Intelligence.

Odpověď:

Ano. Při vyhodnocování příchozího SMTP provozu je využívána reputační databáze Cisco Talos Intelligence.

Další externí reputační databáze nebo blacklisty nejsou samostatně využívány.

---

5. Právní a organizační podklad

Otázka:

Uveďte, který útvar Ministerstva vnitra rozhodl o zavedení mechanismu automatického odmítání příchozích e-mailových zpráv a na základě jakého rozhodnutí nebo dokumentu byl tento mechanismus zaveden.

Odpověď:

Dostupná technická a provozní dokumentace dokládá využívání kontroly DNS v rámci provozu služby nejméně od roku 2019.

Povinnému subjektu nebyly dohledány dokumenty, ze kterých by bylo možné přesně určit datum zavedení tohoto mechanismu ani dokumenty zachycující jeho změny v požadovaném rozsahu.

---

6. Vztah ke zveřejněným podmínkám elektronické podatelny

Otázka:

Uveďte, na základě kterého konkrétního zveřejněného pravidla byla zpráva odmítnuta.

Odpověď:

Zpráva nebyla odmítnuta na základě konkrétního zveřejněného pravidla elektronické podatelny. Jak je uvedeno v odpovědi na otázku č. 3, kontrola příchozího SMTP provozu je realizována prostřednictvím technických mechanismů služby elektronické pošty a bezpečnostních funkcí využívaného produktu Cisco.

---

7. <u>Kontrola falešně pozitivních výsledků</u>

Otázka:

Uveďte, jaký mechanismus Ministerstvo vnitra používá pro zjišťování a nápravu případů, kdy je legitimní zpráva automaticky odmítnuta.

Odpověď:

Kontroly příchozího SMTP provozu jsou prováděny automatizovanými technickými prostředky v rámci provozu elektronické pošty. Rozhodování o důvěryhodnosti (reputaci) zdrojů elektronické pošty je realizováno prostřednictvím interních mechanismů bezpečnostního produktu Cisco.

Ministerstvo vnitra neprovádí běžné individuální posuzování jednotlivých SMTP spojení před jejich přijetím. Pokud je však Ministerstvu vnitra doručen konkrétní podnět týkající se možného nesprávného odmítnutí elektronické zprávy, lze příslušný případ individuálně prověřit odpovědnými pracovníky na základě dostupných provozních záznamů a dalších dostupných informací.

---

8. IP adresa 

Otázka:

Uveďte informace týkající se IP adresy 

Odpověď:

Ministerstvo vnitra disponuje informací, že IP adresa  *byla v souvislosti se zpracováním příchozí elektronické pošty vyhodnocována prostřednictvím bezpečnostních mechanismů využívaných při provozu elektronické pošty.*

Posouzení důvěryhodnosti (reputace) IP adres je realizováno prostřednictvím interních mechanismů bezpečnostního produktu Cisco. Povinný subjekt nedisponuje dokumentací obsahující konkrétní algoritmy, pravidla ani kritéria používaná tímto produktem pro vyhodnocování jednotlivých IP adres.

Další informace vztahující se ke konkrétní IP adrese  *nebyly dohledány.*

---

9. Rozsah odmítání zpráv

Otázka:

Uveďte počet e-mailových zpráv odmítnutých z důvodu reputačního hodnocení, DNS kontrol nebo obdobných bezpečnostních mechanismů v letech 2025 a 2026.

Odpověď:

Ministerstvo vnitra neeviduje statistický přehled počtu e-mailových zpráv odmítnutých z důvodu reputačního hodnocení, DNS kontrol nebo obdobných bezpečnostních mechanismů v členění požadovaném v žádosti.

Požadovaná informace není součástí existujících evidencí ani výstupů povinného subjektu. Její poskytnutí by vyžadovalo vytvoření nové informace dodatečným zpracováním provozních záznamů, k čemuž povinný subjekt není podle zákona č. 106/1999 Sb. povinen.

Povinný subjekt proto požadovanou informací nedisponuje.

---

10. Známé případy legitimních podání

Otázka:

Uveďte, zda Ministerstvo vnitra eviduje případy, kdy byla automaticky odmítnuta e-mailová zpráva obsahující žádost podle zákona č. 106/1999 Sb. nebo jiné úřední podání, a pokud ano, uveďte jejich počet za roky 2025 a 2026.

Odpověď:

Ministerstvo vnitra neeviduje případy, kdy byla automaticky odmítnuta e-mailová zpráva obsahující žádost podle zákona č. 106/1999 Sb. nebo jiné úřední podání.

V případě odmítnutí SMTP spojení před přijetím elektronické zprávy Ministerstvo vnitra nedisponuje obsahem takové zprávy, a nemůže proto zpětně ověřit, zda obsahovala žádost podle zákona č. 106/1999 Sb. nebo jiné úřední podání.

Ministerstvo vnitra současně nevede evidenci, z níž by bylo možné zjistit počet případů požadovaných v žádosti za roky 2025 a 2026.

---

11. <u>Změny pravidel</u>

Otázka:

Poskytněte existující dokumenty zachycující změny pravidel automatického odmítání zpráv od [redacted]

Odpověď:

Povinnému subjektu nebyl dohledán samostatný dokument, který by upravoval nebo zaznamenával změny mechanismu kontroly DNS, reputačního hodnocení nebo obdobných bezpečnostních mechanismů využívaných při zpracování příchozího SMTP provozu.

Informace uvedená v odpovědi na otázku č. 5 vyplývá z dostupné technické a provozní dokumentace. Povinnému subjektu však nebyly dohledány podklady, ze kterých by bylo možné dovodit, že od [redacted] do dne vyřízení žádosti došlo ke změně mechanismu kontroly DNS.

[redacted]