Národní knihovna
České republiky
National Library
of the Czech Republic

Povinná ochrana emailové komunikace

Národní úřad pro kybernetickou a informační bezpečnost

Národní knihovna
České republiky
National Library
of the Czech Republic

Úvod

- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal na základě zákona o kybernetické bezpečnosti v říjnu 2021 ochranné opatření formou veřejné vyhlášky, které se týká zabezpečení poštovních serverů.
- Dle toho opatření jsou všechny orgány a osoby uvedené v §3 písm. c) až f) zákona o kybernetické bezpečnosti splnit následující požadavky.
- Termín splnění těchto požadavků byl stanoven pro některé orgány a osoby na 1. ledna 2022, pro jiné pak nejpozději do 1. července 2022.

Národní knihovna
České republiky
National Library
of the Czech Republic

Požadavky na zabezpečení

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, jejichž elektronická pošta je součástí informačního nebo komunikačního systému, na který se vztahují požadavky zákona o kybernetické bezpečnosti, zajistí, aby při přijímání a odesílání elektronické pošty protokolem SMTP mimo vnitřní síť byly splněny následující požadavky:

Národní knihovna
České republiky
National Library
of the Czech Republic

1. Standardy IETF RFC 3207

- Všechny SMTP servery uvedené v MX záznamech, přes které je přijímána elektronická pošta, a hraniční SMTP servery, přes které je pošta odesílána, podporují zabezpečené spojení dle standardu STARTTLS (IETF RFC 3207)
- Všechny hraniční **SMTP** servery, přes které je **odesílána** elektronická **pošta**, při překladu DNS záznamů **validují** záznamy pomocí technologie **DNSSEC**, pokud jsou touto technologií digitálně podepsány. **Nevalidně podepsané záznamy jsou ignorovány**. Pokud je validace prováděna pomocí DNS serveru, validující DNS server se musí nacházet na stejném serveru nebo ve stejné síti jako SMTP server či využívat spojení, které zabezpečí integritu přenosu.

Národní knihovna
České republiky
National Library
of the Czech Republic

2. Podporované protokoly

- V rámci zabezpečeného spojení všechny servery, přes které je přijímána nebo odesílána elektronická pošta:
- Podporují protokol TLSv1.2 nebo novější
- Nepodporují protokol SSLv3 a starší
- Podporují protokoly TLSv1.0 a TLSv1.1 pouze v odůvodněných nezbytných případech, kdy by omezení podpory těchto protokolů mohlo způsobit omezení dostupnosti a řádného fungování systému elektronické pošty.
- Používají v rámci TLS spojení kryptografické prostředky, které jsou aktuálně odolné dle doporučení Úřadu vydávaného v návaznosti na § 26 písm. d) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Jiné prostředky mohou být použity pouze v odůvodněných případech.

Národní knihovna
České republiky
National Library
of the Czech Republic

3. Certifikáty pro SMTP

- Certifikáty všech SMTP serverů uvedených v MX záznamech jsou validní, vystaveny uznávanou certifikační autoritou a s doménovým názvem odpovídající názvu MX záznamu daného serveru
- **Všechny** hraniční **SMTP** servery, přes které je **odesílána** elektronická pošta, **ověřují** certifikát protistrany pomocí **TLSA** záznamu, pokud jej protistrana zveřejnila. V případě, že otisk certifikátu neodpovídá nabídnutému certifikátu vzdáleného serveru nebo vzdálený server nepodporuje navázání zabezpečeného spojení, elektronická pošta **nebude** na tento server **odeslána**.

Národní knihovna
České republiky
National Library
of the Czech Republic

4. DNS a DNSSEC

- Všechny DNS záznamy relevantní pro funkci přijímání pošty mají zabezpečenou integritu pomocí technologie DNSSEC (IETF RFC 4033). Kryptografické algoritmy použité pro digitální podpis DNS záznamů musí být aktuálně odolné.
- Všechny tyto domény musí být podepsány u registrátorů domén prvního řádu.

Národní knihovna
České republiky
National Library
of the Czech Republic

5. TLSA záznam v DNS dle technologie DANE

- Všechny používané MX záznamy SMTP serverů mají zveřejněn odpovídající TLSA záznam v DNS dle technologie DANE