Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

PŘÍLOHA K Č.J. 8477/2021-NÚKIB-E/350 • BRNO • 11. ŘÍJNA 2021

VERZE DOKUMENTU: 1.0

METODIKA K ZAVEDENÍ ZPŮSOBŮ ZVÝŠENÍ OCHRANY DLE OCHRANNÉHO OPATŘENÍ ZE DNE 11. 10. 2021

1 Úvod

Tento dokument poskytuje metodický návod k zavedení zvýšení ochrany e-mailové komunikace vyplývající z ochranného opatření, které Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) vydal dne 11. 10. 2021. Toto ochranné opatření vydané na základě § 14 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, stanovuje způsoby zvýšení ochrany informačních systémů a směřuje k zajištění důvěrnosti a integrity elektronické pošty a k zamezení podvržení elektronické pošty při komunikaci mezi povinnými osobami dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti. Zvláštní důraz je pak kladen na zajištění bezpečné komunikace mezi orgány veřejné moci, které se budou podílet na předsednictví České republiky v rámci Rady EU.

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Popis problému

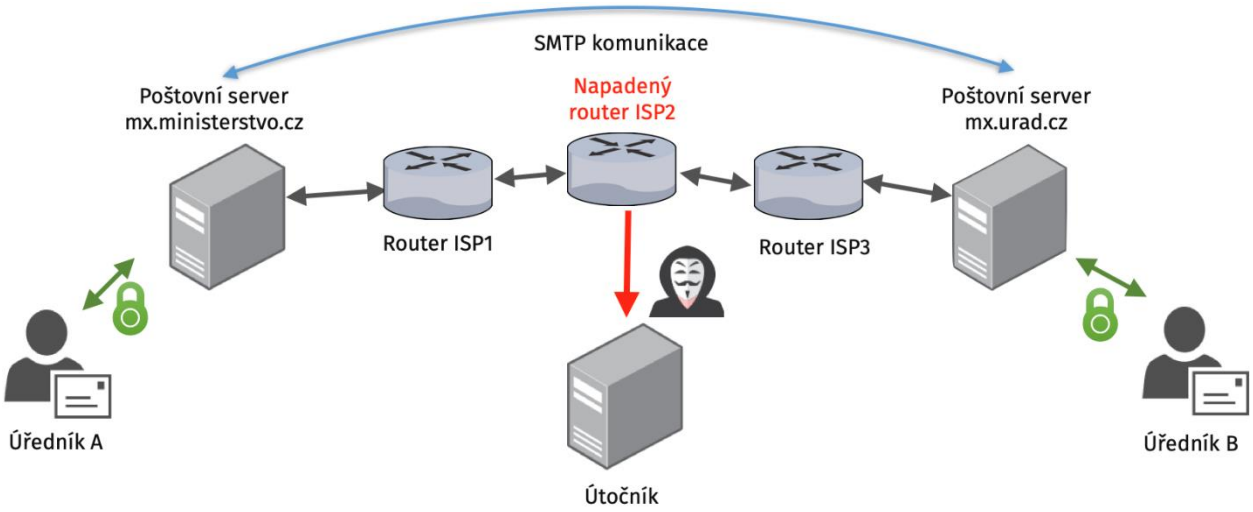
Útoky typu *Man-in-the-middle* (MITM) fungují tak, že se útočník dostane do pozice prostředníka mezi komunikujícími subjekty a má tak možnost narušovat důvěrnost a integritu komunikace, pokud není zajištěna jinými prostředky.

STARTTLS je zpětně kompatibilní způsob, jakým můžou komunikující strany navázat zabezpečené spojení pomocí kryptografického protokolu TLS na původně textovém protokolu jako je například SMTP.

Při odesílání poštovní zprávy ze SMTP serveru (C) na jiný SMTP server (S) je nejprve navázána nezabezpečená komunikace. Následně SMTP server zašle zprávu informující o podporovaných rozšířeních – pokud server podporuje STARTTLS, obsahuje tato zpráva tento řetězec. Pokud i SMTP server, který zprávu odesílá, podporuje toto rozšíření, odpoví zprávou STARTTLS a započne navazování zabezpečeného spojení.

```
S: 220 mail.example.org ESMTP service ready
C: EHLO client.example.org
S: 250-mail.example.org offers a warm hug of welcome
S: 250 STARTTLS
C: STARTTLS
S: 220 Go ahead
```

Toto řešení zabezpečení brání pouze pasivnímu útoku typu MITM, kdy útočník nemá možnost nebo nechce měnit komunikaci, ale pouze ji odposlouchávat. V případě, že má útočník přístup k jakémukoliv prvku nacházející se mezi dvěma komunikujícími SMTP servery (tedy i mimo infrastrukturu organizace) a má možnost měnit komunikaci, může jednoduchým způsobem upravit oznámení serveru a vynechat informaci o podpoře STARTTLS. Spojení tak nebude povýšeno na zabezpečené a útočník může přistupovat k přenášené komunikaci, a tedy i odesílaným nebo přijímaným zprávám (pokud nejsou šifrovány pomocí end-to-end šifrování jako je S/MIME nebo PGP). Případně je může i upravovat, aniž by takovou úpravu bylo možné detekovat (pokud nejsou zprávy digitálně podepsány pomocí DKIM, S/MIME nebo PGP).



Obrázek 1 Schematické znázornění útoku typu MITM

Nastavit SMTP server tak, aby vždy vyžadoval navázání zabezpečeného spojení, a tedy v případě neexistence značky STARTTLS nepokračoval v komunikaci není prakticky možné, neboť v současné době podporuje STARTTLS pouze 90 % SMTP serverů[1] a některé zprávy by tak nebylo možné přijmout nebo doručit.

I pokud by bylo vynuceno navázání zabezpečeného spojení vždy, problém by to nevyřešilo, jen případnému útočníku ztížilo práci. Při standardním nastavení SMTP server totiž nekontroluje, zda je serverový certifikát protistrany validní, jakou certifikační autoritou je vydán nebo zda je vydán pro doménu SMTP serveru. Toto výchozí chování je tedy odlišné, než u přístupu k webovým stránkám, kde prohlížeče v takovém případě zobrazí uživatelům výrazné upozornění, případně ani neumožní takovou stránku navštívit. Pokud by útočník podvrhl použitý certifikát za jakýkoliv jiný (např. i *self signed*), spojení by i tak bylo navázáno.

Vynutit kontrolu certifikátu je sice technicky možné (některé SMTP servery takové nastavení umožňují), opět by to ale vedlo k nedoručitelnosti některých e-mailů nebo by byly zasílány nezabezpečeně, jelikož 23 % SMTP serverů nepoužívá platný certifikát.[2]

Řešením tohoto problému spočívá v informování protistrany jiným kanálem, že tento SMTP server podporuje STARTTLS a má platný certifikát. Pokud při navazování komunikace nebude jedna z těchto podmínek splněna, komunikace nebude navázána, a útočník tak nebude moci zprávy odposlechnout nebo měnit (nebo to pro něj bude o mnoho složitější).

Takto funguje technologie DANE, kdy je v rámci digitálně podepsaných DNS záznamů zveřejněn otisk použitého certifikátu SMTP serveru. Při vytváření spojení se nejprve ověří, zda je v rámci DNS zveřejněn otisk certifikátu v rámci TLSA záznamu. V případě, že je tento otisk zveřejněn a vzdálený server neoznámí podporu STARTTLS nebo certifikát nebude odpovídat otisku z TLSA záznamu, spojení nebude navázáno. Pokud tedy případný útočník bude modifikovat komunikaci

[1] Dle statistik společnosti Google, dostupné na https://transparencyreport.google.com/safer-email/overview?hl=cs
[2] Dle statistik z nástroje MECSA, dostupné na https://mecsa.jrc.ec.europa.eu/en/stats

a odstraňovat řetězec STARTTLS při navazování spojení nebo podvrhovat certifikát serveru, bude ochráněna důvěrnost i integrita přenášených zpráv.

Na zabezpečení komunikace mezi SMTP servery se zaměřuje první část výroku opatření. Druhá část se zaměřuje na obdobný problém (tedy zabránění útoků typu MITM), ale v rámci komunikace mezi klientem elektronické pošty a poštovním serverem.

Aby mohla technologie DANE fungovat, musí ji podporovat jak strana odesilatele, tak strana příjemce. Rozšíření této technologie však ještě není nedostatečné (v současné době jedná o 16 % domén[3]), i když předpokládáme, že bude postupně narůstat. Třetí část opatření proto alespoň míří na zajištění integrity přenášené zprávy elektronické pošty, pokud jedna z komunikujících stran nepodporuje technologii DANE.

DKIM umožňuje digitálně podepsat určité části zprávy (určené hlavičky a tělo zprávy) pomocí asymetrické kryptografie. Soukromý klíč je využit pro podepsání zprávy, veřejný je uložen v určeném DNS záznamu. Pokud tedy útočník upraví přenášenou zprávu, digitální podpis nebude platný. Pro informování, jak má server příjemce naložit s nepodepsanou nebo nevalidně podepsanou zprávou slouží technologie DMARC.

[3] Dle statistik z nástroje MECSA, dostupné na https://mecsa.jrc.ec.europa.eu/en/stats

3 Doporučení postupu při implementaci

3.1 Jak začít

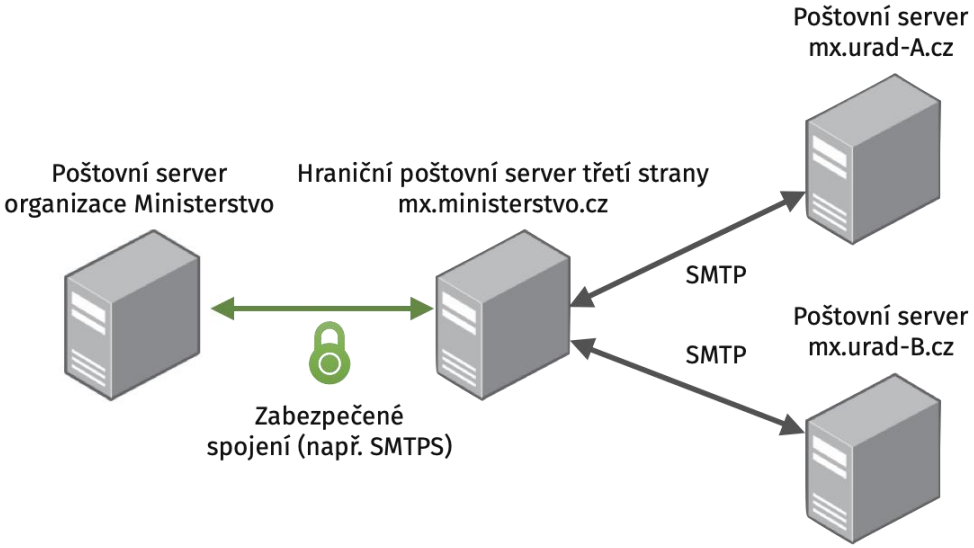
- Prvním krokem při implementaci by měla být inventura veřejných doménových jmen organizace, které organizace vlastní nebo využívá. Z těchto domén by měly být identifikovány ty, které se používají pro zasílání nebo příjem elektronické pošty.
- Doména určená pro příjem pošty je taková, která má ve veřejném DNS vystaven alespoň jeden MX záznam.
- Seznam MX záznamů pro určitou doménu lze získat pomocí příkazu `dig mx example.com` dostupného na většině linuxových distribucí, nebo v interaktivním módu nástroje `nslookup`:
  - nastavit > `set type=MX`
  - a poté zadat žádanou doménu > `example.com.`
- Doména určená pro odesílání pošty je taková, která se vyskytuje v hlavičce *From* nebo se používá v *envelope-from*.
- Domény, které organizace vlastní a nejsou používány pro odesílání pošty, by měly mít nastaven SPF a DMARC záznam, který zablokuje zasílání pošty z těchto domén (viz níže), aby nemohly být zneužity případným útočníkem.
- Zavedení opatření je vyžadováno pouze mimo vnitřní síť, přesto však relevantní opatření doporučujeme zavést i v rámci vnitřní sítě.

3.2 Služby třetích stran pro kontrolu pošty

Některé organizace využívají službu třetích stran pro kontrolu přijímané a odesílané pošty (SMTP gateway). Tyto nástroje umožňují mimo jiné např. implementovat některé požadované opatření, odstraňovat nebo označovat škodlivou poštu nebo spam. V případě, že organizace takový nástroj využívá, nebo se rozhodne využít, je možné požadované opatření implementovat pomocí SMTP gateway.

V takovém případě je ale nutné zajistit, aby komunikace mezi SMTP serverem organizace a SMTP gateway nemohla být ponížena na nezabezpečenou, pokud tato komunikace probíhá mimo interní síť, a to jak při odesílání, tak příjmu pošty (viz bod 1.8 výroku opatření). Tohoto lze docílit více způsoby, např.:

- Využití SMTPS protokolu s autentizací obou stran.
- Vynucení STARTTLS u SMTP protokolu s kontrolou certifikátu (nedoporučováno).
- Využití jiného protokolu, u kterého nelze ponížit komunikaci na nezabezpečenou.
- Zapouzdření přenášené komunikace do jiného zabezpečeného kanálu (např. VPN).



Obrázek 2 Schematické znázornění využití služby třetí strany

3.3 Co dělat, pokud použitý systém nepodporuje některou z požadovaných technologií?

Ne všechny SMTP servery, případně cloudové služby, podporují všechny technologie, jejichž zavedení vyžaduje toto opatření. V takovém případě vám doporučujeme se obrátit na dodavatele vámi použitého SMTP serveru nebo cloudové služby s žádostí o podporu a implementaci těchto technologií.

Pokud výrobce neplánuje uvedené technologie podporovat nebo je použité řešení již bez podpory a výměna by byla nákladná, je možné využít předsunutý SMTP server, který bude sloužit jako SMTP gateway a který bude podporovat všechny vyžadované technologie. Některé z těchto SMTP serverů jsou dostupné zdarma pod open-source licencí.

Toto řešení lze využít i v případě, že organizace využívá cloudovou službu, která tyto technologie nepodporuje.

V případě pořizování nové technologie nebo cloudové služby doporučujeme požadavky na technologie vyžadované tímto opatřením vhodně zakomponovat do požadavků v rámci zadávacího řízení (pro inspiraci je možné vycházet z bodů uvedených v sekci Checklist opatření).

4 Doporučení pro implementaci jednotlivých technologií

4.1 STARTTLS v rámci SMTP

- Technologie STARTTLS byla vyvinuta jako zpětně kompatibilní způsob, jakým lze navázat zabezpečené spojení na poštovní server.
- Navazování komunikace probíhá nejprve nezabezpečeně v čistém textu. Pokud server STARTTLS podporuje, indikuje to pomocí textové zprávy STARTTLS. Pokud i klient STARTTLS podporuje, vyšle na server zprávu STARTTLS a začne navazovat zabezpečené spojení pomocí TLS.
- Tento způsob se nazývá oportunistické TLS, což znamená, že je náchylné na aktivní MITM útok. Pokud útočník zamezí vytvoření TLS komunikace, klient nenaváže bezpečný kanál a komunikace tak bude probíhat nezabezpečeně – takovou komunikaci pak může útočník odposlouchávat nebo dokonce měnit.
- Pro zamezení navázání zabezpečené komunikaci útočníkovi postačí, aby útočník v nešifrované komunikaci vynechal indikátor STARTTLS, který zasílá server.
- I při využití protokolu STARTTLS většina klientů při navazování spojení nekontroluje, zda poskytnutý certifikát odpovídá danému SMTP serveru. Zabezpečené spojení je tak navázáno i v případě, pokud je certifikát *self signed*, nebo např. vypršený.

4.2 Certifikát

- Vystavený certifikát pro poštovní server musí být podepsaný uznávanou certifikační autoritou, tak aby byl akceptován v nejrozšířenějších systémech (Windows, unixové systémy, macOS, iOS a Android). Seznam obecně uznávaných certifikačních autorit je dostupný na Common CA Database (https://www.ccadb.org). Použitý certifikát certifikační autority musí být dostupný jak v seznamu společnosti Microsoft, tak společnosti Mozilla (certifikáty uznávané společnosti Mozilla jsou přejímány linuxovými operačními systémy a dalšími open-source řešeními).
- V případě certifikátu SMTP serveru určeného pro příjem pošty musí být v sekci *subjectAltName* certifikátu uvedena doména SMTP serveru dle MX záznamu. Například pokud doména *example.com* má uvedený MX záznam *mx.example.com*, musí certifikát SMTP serveru obsahovat v sekci *subjectAltName* doménu *mx.example.com*.
- Datum vypršení certifikátu doporučujeme sledovat pomocí nástrojů třetích stran případně interním monitoringem organizace. Běžně nastává situace, že správce sice provede výměnu certifikátu, ale např. zapomene restartovat aplikační server, aby se změna projevila. Automatické sledování na tuto situaci dokáže upozornit a předejít problém s nedostupností serveru.

4.3 TLS (SSL)

- TLS (Transport Layer Security, starší verze jsou označovány jako SSL) je nejpoužívanější kryptografický protokol určený pro navazování zabezpečené komunikace. Tento protokol se využívá např. v rámci HTTPS, SMTPS, IMAPS apod.
- V současné době jsou považovány za odolné verze protokolů TLSv1.2 a TLSv1.3.
- Některé starší systémy a poštovní servery nemusí podporovat TLSv1.2 a novější. V případě vypnutí starších verzí doporučujeme na serveru nejprve povolit logování použité verze TLS protokolu při navazování spojení a následně zkontrolovat, jaké verze se ve skutečnosti používají.
- V rámci verzí protokolů TLSv1.0 až TLSv1.2 je možné volit podporované kryptografické prostředky pro výměnu klíčů, šifrování a hašovacích funkcí. Zvolené prostředky musí podporovat obě strany, jinak nemůže být spojení navázáno. Tyto prostředky musí být v souladu s doporučením Úřadu.[4] Volit jiné prostředky je možné pouze v nezbytných odůvodněných případech.
- Verze TLSv1.2 a starší umožňuje povolit kompresi. Tato možnost by měla být vypnuta pro zabránění útoků typu CRIME.
- V rámci protokolu TLSv1.3 není možné volit podporované algoritmy – všechny podporované algoritmy využívané tímto protokolem jsou v současné době v souladu s doporučením Úřadu.
- Pro ověření použitých protokolů a kryptografických prostředků v rámci TLS při připojování klienta na server je možné využít např. open-source nástroj `testssl` (https://testssl.sh) určený pro unixové systémy nebo jiné, bezplatné online nástroje (viz níže).

```
> testssl.sh -t smtp –mx example.com
```

4.4 DNSSEC

- Použití DNSSEC při nákupu všech relevantních služeb je pro ministerstva a ostatní ústřední orgány státní správy vyžadováno od 1. ledna 2014 (usnesení vlády 727/2009).
- Mezi aktuálně odolné kryptografické algoritmy u technologie DNSSEC patří:
    - RSASHA256 (algoritmus 8)
    - ECDSAP256SHA256 (algoritmus 13)
    - ECDSAP384SHA384 (algoritmus 14)
    - ED25519 (algoritmus 15)
    - ED448 (algoritmus 16)

[4] Dostupné na https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf

- Zda jsou záznamy podepsány a jakým algoritmem, je možné ověřit pomocí zdarma dostupných online nástrojů (viz níže).
- Validace DNS záznamů je ochranným opatřením vyžadována pouze na hraničním SMTP serveru, přesto však doporučujeme tuto validaci provádět na všech serverech, kterými je doručována nebo přijímána elektronická pošta.
- Ověřit funkční validaci DNSSEC lze např. pokusem o překlad domény `rhybar.cz`. V případě správně nastaveného DNS serveru by měl překlad skončit chybovou zprávou typu SERVFAIL nebo vypršením času.
    - Na systémech typu unix:

      `> dig rhybar.cz`
    - Na systémech Microsoft Windows:

      `> nslookup rhybar.cz`

4.5 DANE

- Funkce technologie DANE spočívá ve zveřejnění otisku certifikátu v rámci DNS záznamu typu TLSA. Při odesílání poštovní zprávy odesílající server ověří, zda protistrana má TLSA záznam zveřejněn, a pokud ano, zkontroluje, zda zveřejněný otisk certifikátu odpovídá certifikátu předanému při navazování TLS spojení.
- Pro vytvoření TLSA záznamu lze využít volně dostupné nástroje.
- TLSA záznam musí být pro správnou funkci podepsán DNSSEC, jinak může být protistranou ignorován.
- V případě výměny certifikátu poštovního serveru je třeba změnit taktéž TLSA záznam. Proto doporučujeme nastavit TTL pro TLSA záznam s nízkou dobou životnosti (jednotky minut). V případě plánované výměny certifikátu je možné využít duplicitního záznamu, kdy bude v DNS existovat záznam jak pro současný, tak budoucí certifikát. V případě duplicitních záznamů stačí, aby odpovídal alespoň jeden z nich použitému certifikátu.
- Ověření správnosti nastavení TLSA je možné například pomocí nástroje `posttls-finger`, který je součástí open-source mailového serveru postfix, nebo pomocí bezplatných online nástrojů.
- TLS Reporting (TLS-RPT, IETF RFC 8460) je nástroj, díky kterému se může správce SMTP serveru dozvědět, zda je v pořádku navazováno TLS spojení z ostatních SMTP serverů (např. v případě nevalidního certifikátu). Doporučujeme tento nástroj využít pro zajištění dostupnosti. Pro vyhodnocování TLS-RPT je možné využít služby třetích stran.

4.6 MTA-STS

- MTA-STS (IETF RFC 8461) je komplementární technologií pro DANE, které plní obdobnou funkci, ale jinými prostředky.
- Tato technologie vznikla později než DANE a řeší problém, pokud není možné využít DNSSEC.
- Namísto zveřejnění otisku použitého certifikátu je zveřejněn DNS záznam a soubor na webové stránce, který informuje poštovní server o nutnosti využít zabezpečené spojení.
- Vzhledem k tomu, že DNS záznam u technologie MTA-STS nemusí být podepsán technologií DNSSEC, případný útočník má možnost při podvržení komunikace tento záznam „zatajit" – proto tato technologie není tak bezpečná jako DANE.
- Podpora pro tuto technologii taktéž není tak rozšířená (interní výzkum Úřadu).
- Zavedení této technologie tedy pouze doporučujeme pro zvýšení bezpečnosti po zavedení DANE, ochranným opatřením však není zavedení této technologie vyžadováno.

4.7 HSTS

- HTTP Strict Transport Security je mechanismus, který umožňuje klientovi z pohledu serveru určit, že pro přístup k určitým webovým stránkám se má využívat výhradně zabezpečené připojení přes protokol HTTPS.
- Pokud daný systém hlavičku neumožňuje nastavit, je možné ji nastavit pomocí webového serveru nebo na reverzní proxy.
- Parametr *max-age* určuje, po jakou dobu si má klient pamatovat, že má využívat výhradně zabezpečené spojení. Při zavádění této technologie doporučujeme tento čas nastavit na kratší dobu a případně jej postupně navýšit až na doporučovanou hodnotu 10368000 sekund (120 dní) a více.
- V případě vypršení certifikátu neumožní prohlížeč schválit bezpečnostní výjimku a pokračovat v používání stránky. Proto doporučujeme automatizovaně sledovat datum vypršení certifikátu (viz sekce Certifikát).

4.8 SPF

- Technologie SPF (Sender Policy Framework) umožňuje organizaci definovat, které SMTP servery mohou posílat elektronické poštovní zprávy z domény organizace.
- Zobrazit existující SPF záznam pro doménu lze pomocí příkazu `dig` nebo `nslookup`. SPF záznam začíná hodnotou v=spf1.

```
> dig txt example.com
> nslookup -type=txt example.com
```

- Při prvotním nastavení SPF doporučujeme volit politiku *?all*. Nastavení přísnější politiky je doporučení až po nastavení DMARC a získání reportů.
- V případě, že SMTP server podporuje IPv6, je pro správné fungování potřeba uvést do SPF záznamu i IPv6 adresy nebo rozsahy.
- Zpočátku doporučujeme nastavit pro DNS záznam nízkou hodnotu TTL (v řádech minut), aby mohla být případně špatná konfigurace záznamu rychle opravena.
- Pokud instituce vlastní domény, které nepoužívá k zasílání pošty, doporučujeme zablokovat zasílání e-mailů z těchto domén pomocí SPF záznamu `v=spf1 ~all` nebo `v=spf1 -all`.
- Vždy je třeba ověřit, zda dané domény nejsou využívány pro zasílání elektronických poštovních zpráv z jiných serverů: typicky registrační e-maily, notifikační e-maily nebo různé newslettery. V takovém případě je potřeba dané servery zařadit do SPF záznamu.

4.9 DKIM

- DKIM funguje na principu asymetrické kryptografie, kdy jsou určené hlavičky a text zprávy digitálně podepsány. Veřejný klíč je zveřejněn v rámci k tomu určeného DNS záznamu, privátní klíč nesmí opustit SMTP server.
- V případě využití více SMTP serverů pro odesílaní pošty může každý SMTP server využívat vlastní dvojici klíčů zveřejněné pod rozdílnými selektory.
- Při podepisování doporučujeme využít algoritmus `rsa-sha256`. Algoritmus `rsa-sha1` byl označen jako zastaralý v roce 2018 (IETF RFC 8301). Algoritmus `ed25519-sha256` definovaný v IETF RFC 8463 není v současné době široce podporován.
- Pro podepisování doporučujeme využít RSA klíč o velikosti 2048 bitů. Klíč o vyšší velikosti nedoporučujeme využít, jelikož původní verze IETF RFC 6376 z roku 2011, vyžadovala podporu pouze pro klíče o velikosti 1024 a 2048 bitů, protistrana tak nemusí klíč o této velikosti ještě podporovat.
- Při podepisování je možné zvolit hlavičky, které mají být podepsány. Ochranné opatření vyžaduje podepsání alespoň hlaviček *From* a *Subjet*. Pro volbu dalších hlaviček doporučujeme vycházet z kapitoly 5.4.1 v IETF RFC 6376.
- Jak se má server zachovat, pokud je mu doručena zpráva bez podpisu nebo s nevalidním podpisem, určuje DMARC (viz níže).
- Pro některé SMTP servery jsou k dispozici bezplatné pluginy třetích stran, které přidávají podporu pro tuto technologii.

4.10 DMARC

- Technologie DMARC (Domain-based Message Authentication Reporting and Conformance) podrobněji definuje, jak má server příjemce naložit se zprávou, která

nebyla podepsána pomocí DKIM, či je DKIM podpis neplatný, nebo byla zaslána z jiného než určeného SMTP serveru dle SPF záznamu.

- Získat DMARC záznam pro doménu lze pomocí příkazu `dig` nebo `nslookup`. DMARC záznam začíná hodnotou `v=DMARC1`.
  > `dig txt _dmarc.example.com`
  > `nslookup -type=txt _dmarc.example.com`.
- Nastavení SPF a DKIM by mělo předcházet nastavení DMARC alespoň o 48 hodin.
- Parametr `sp` určuje, jakým způsobem má vzdálený SMTP server naložit s e-mailovou zprávou doručenou ze subdomény. Pokud není uveden, použije se hodnota uvedená v parametru p. Doporučujeme tedy tuto hodnotu neuvádět, aby se politika DMARC p vztahovala i na e-mailové zprávy doručené ze subdomén.
- Parametr `rua` specifikuje e-mailovou adresu, na kterou budou zasílány DMARC reporty. Tyto reporty obsahují informace zasílané z ostatních SMTP serverů a dokážou identifikovat problémy se špatným nastavením SPF, DKIM a DMARC. Pro vyhodnocování DMARC reportů je možné využít služby třetích stran.
- Při zavádění DMARC je vhodné zpočátku nastavit hodnotu parametru p na `none` po dobu přibližně dvou měsíců, během kterých jsou vyhodnocovány doručené DMARC reporty.
- Pokud instituce má ve správě domény, které nepoužívá k zasílání pošty, doporučujeme zablokovat zasílání e-mailů pomocí DMARC záznamu s hodnotou parametru p nastaveným na `reject`.

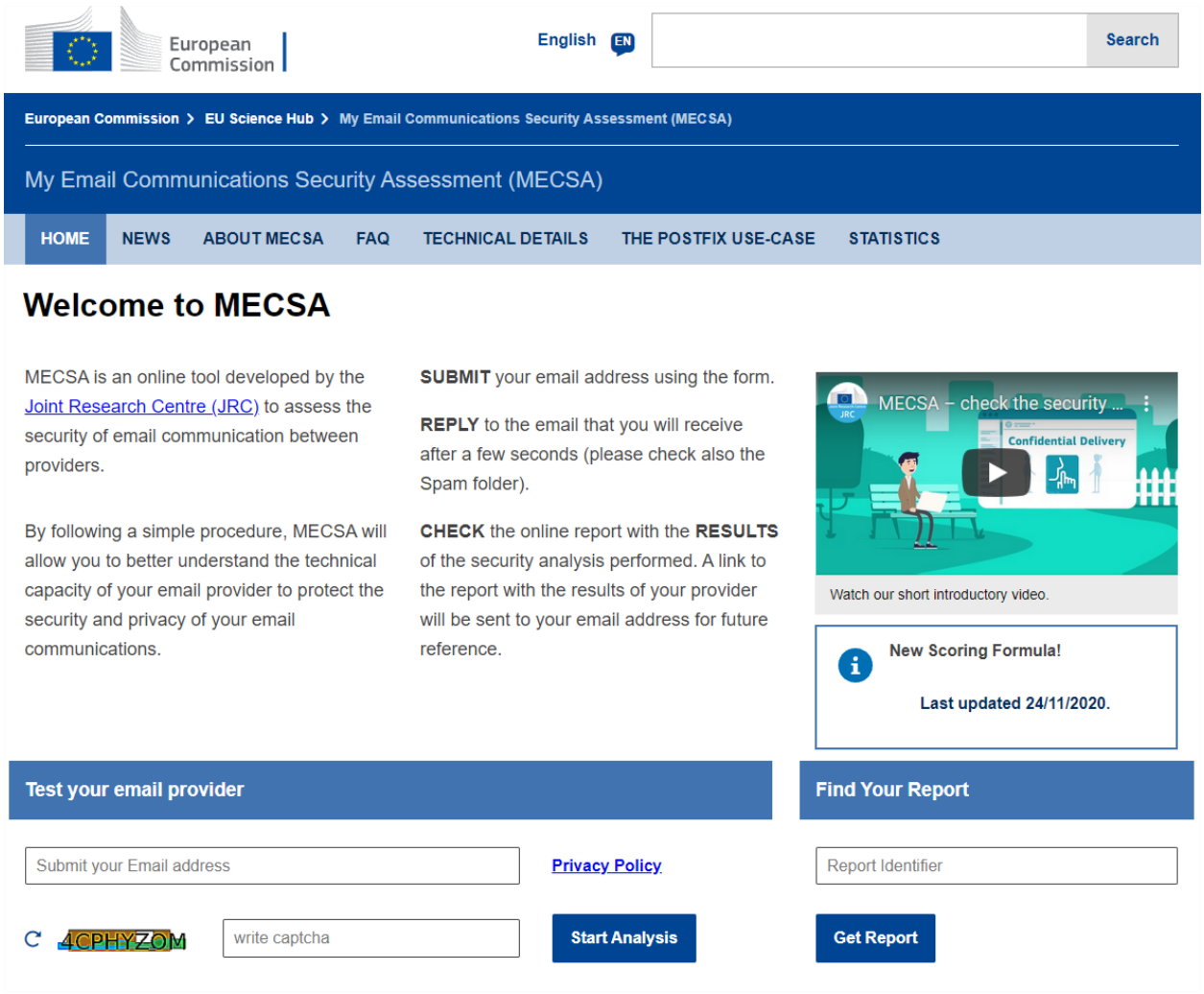
5 Nástroje na orientační ověření některých bodů opatření

Upozornění:

Tyto nástroje nejsou vytvářeny ani spravovány Úřadem a můžou se měnit v čase. Jsou vhodné pouze pro orientační ověření nastavení určitých parametrů poštovního serveru. Úřad nemůže jakkoli garantovat správnost zjištěných výsledků.

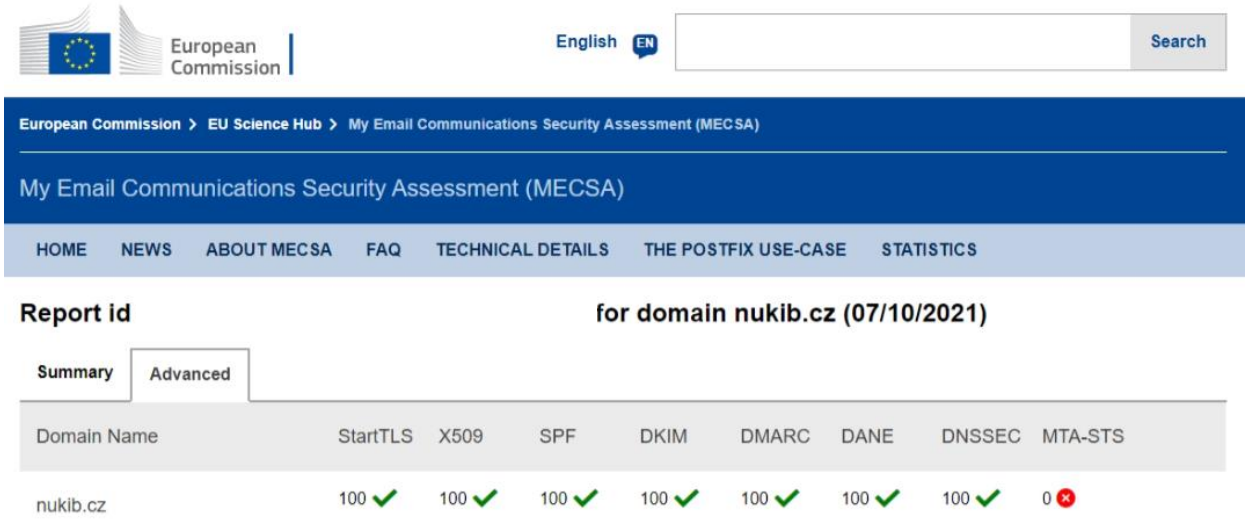
5.1 My Email Communications Security Assessment (MECSA)

MECSA (https://mecsa.jrc.ec.europa.eu/en/) je nástroj vytvořený Evropskou komisí a slouží k ověření zabezpečení e-mailové komunikace, a to jak při příjmu, tak při odesílání elektronické pošty. Pro ověření nastavení je potřeba zadat e-mailovou adresu do pole *Test your email* provider, ke které má uživatel přístup a nachází se na doméně organizace, a vyplnit CAPTCHA.



Obrázek 3 Úvodní stránka MECSA

Na vyplněnou adresu bude následně poslán e-mail, na který je potřeba odpovědět (není nutné vyplňovat text zprávy). Po přijetí zprávy je zobrazen výsledek testu.



Obrázek 4 Ukázka výsledku testu

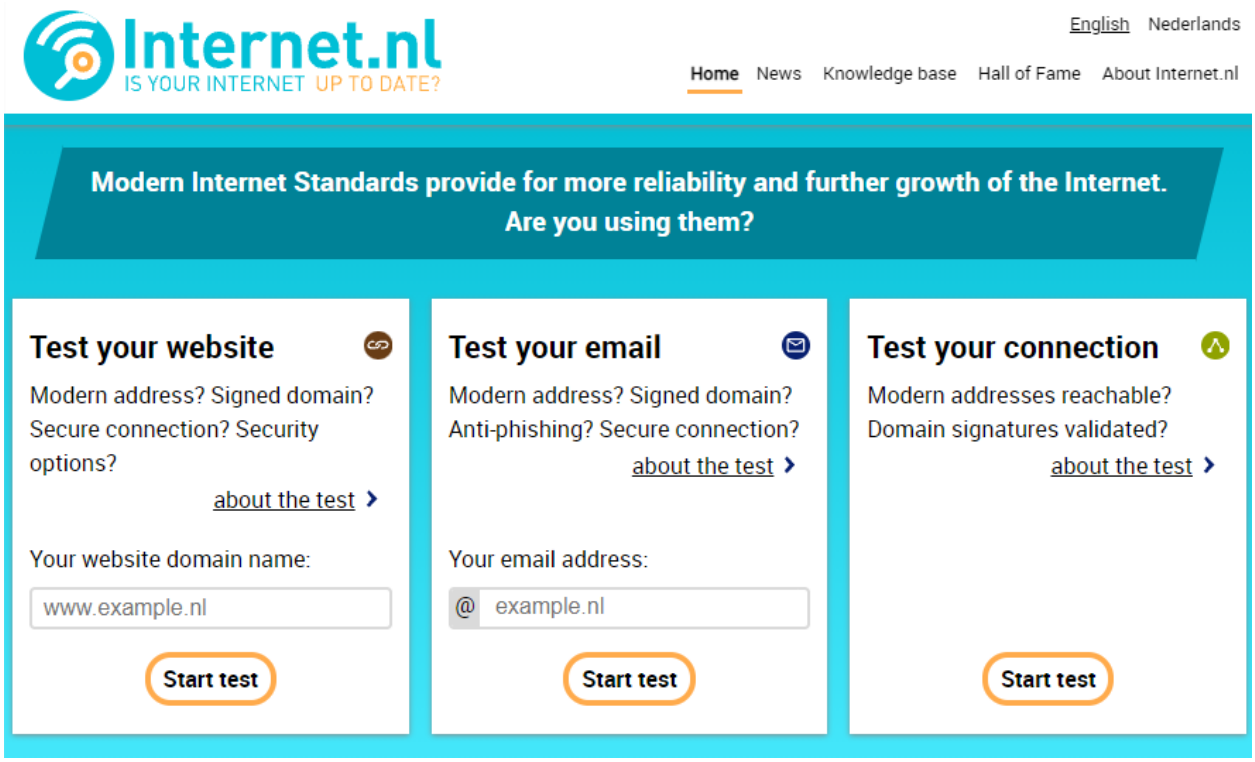
Správně nastavený server by měl obsahovat plný počet (100) bodů ve všech kategoriích v sekci *Advanced*, kromě kategorie MTA-STS, která není ochranným opatřením vyžadována.

Ani získání plného bodů v určité kategorii ale neznamená, že organizace plní všechny body z ochranného opatření.

5.2 Internet.nl

Některé body opatření lze orientačně ověřit pomocí online nástroje internet.nl (https://internet.nl/), což je iniciativa nizozemské vlády a internetové komunity, která má za cíl zvýšit bezpečnost internetové komunikace.

Pro spuštění testu postačí do pole *Test your email* vložit doménu použitou pro příjem a odesílání elektronické pošty a následně stisknout tlačítko *Start test*.



Obrázek 5 Úvodní stránka projektu Internet.nl

Po několika sekundách po provedení testu jsou zobrazeny výsledky. Ne všechny body, které tento test ověřuje, jsou však vyžadovány tímto ochranným opatřením, a naopak test neověřuje všechny body vyžadované ochranným opatřením. Následující testy orientačně ověřují tyto výroky opatření:

- *Signed domain names (DNSSEC)* – bod 1.4
- *Authenticity marks against phishing (DMARC, DKIM and SPF)* – body 3.1, 3.2, 3.3
- *Secure mail server connection (STARTTLS and DANE)*
    - *TLS: STARTTLS* – bod 1.1 při příjmu elektronické pošty
    - *TLS: TLS version* – bod 1.2 při příjmu elektronické pošty
    - *Certificate* – bod 1.3
    - *DANE* – bod 1.6

6 Checklist opatření

6.1 Opatření pro zajištění důvěrnosti a integrity komunikace mezi poštovními servery

- SMTP servery uvedené v rámci MX záznamů domény umožňují příjem pošty přes STARTTLS.
- SMTP server má vypnuto SSLv3 a starší při příjmu pošty.
- SMTP server má vypnuto TLSv1.0 a TLSv1.1 při příjmu pošty (výjimka je možná).
- SMTP server podporuje TLSv1.2 nebo novější při příjmu pošty.
- SMTP server používá pouze kryptografické prostředky dle doporučení Úřadu (výjimky jsou možné) při příjmu pošty.
- Certifikát SMTP serveru je validní a je vystaven uznávanou certifikační autoritou.
- Hraniční SMTP server při odesílání pošty využívá STARTTLS, pokud protistrana deklaruje podporu STARTTLS při navazování spojení.
- SMTP server při odesílání pošty nevyužívá protokol SSLv3 a starší.
- SMTP server při odesílání pošty nevyužívá protokol TLSv1.0 a TLSv1.1 (výjimka je možná).
- SMTP server při odesílání pošty využívá protokol TLSv1.2 nebo novější.
- SMTP server při odesílaní pošty využívá pouze kryptografické prostředky dle doporučení Úřadu (výjimky jsou možné).
- Hraniční SMTP server validuje DNSSEC, nebo se validující DNS server nachází přímo na SMTP serveru, ve stejné síti, nebo je komunikace mezi SMTP serverem a DNS serverem zabezpečena (VPN, DNS-over-TLS, DNS-over-HTTPS apod.).
- Všechny DNS záznamy typu A, AAAA, MX a TLSA serverů použitých pro příjem pošty jsou podepsány technologií DNSSEC.
- MX záznamy všech SMTP serverů obsahují TLSA záznam, který odpovídá použitému certifikátu.
- Hraniční SMTP server při odesílání pošty ověřuje TLSA záznam protistrany dle IETF RFC 7672.
- Komunikace mezi definovanými SMTP servery musí být zabezpečena aktuálně odolnými kryptografickými prostředky, dále musí být zajištěna nemožnost ponížení komunikace na nešifrovanou a obě strany musí zajistit ověřování autenticity protistrany (obvykle využitím protokolu SMTPS).

6.2 Opatření pro zajištění důvěrnosti a integrity komunikace mezi klientem elektronické pošty a serverem

- Všechna spojení z koncových zařízení na poštovní server, který se nachází v jiné síti, jsou zabezpečena.
- Poštovní server používá pro zabezpečení spojení s koncovým zařízením pouze kryptografické prostředky dle doporučení Úřadu při příjmu a odesílání pošty (výjimky jsou možné).
- Poštovní server má vypnuto SSLv3 a starší.
- Poštovní server má vypnuto TLSv1.0 a TLSv1.1 (výjimka je možná).
- Poštovní server podporuje TLSv1.2 nebo novější.
- Certifikáty poštovního serveru jsou validní a jsou vystaveny uznávanou certifikační autoritou. Pokud certifikáty nejsou vystaveny uznávanou certifikační autoritou, použitá certifikační autorita je dostupná ve všech zařízeních, které se na poštovní server připojují.
- Při použití protokolu SMTP pro odesílání pošty je povolen pouze SMTPS (obvykle port 465).
- Při použití protokolu POP3 pro příjem pošty je povolen pouze POP3S (obvykle port 995).
- Při použití protokolu IMAP pro příjem pošty je povolen pouze IMAPS (obvykle port 993).
- V případě použití protokolu HTTP nebo protokolu založeném na HTTP je povolen pouze protokol HTTPS.
- V případě přístupu přes protokol HTTP je nastavena HTTP hlavička *Strict-Transport-Security* s hodnotou parametru *max-age* větším než nula.

6.3 Opatření pro zajištění integrity a zamezení podvržení odesilatele elektronické poštovní zprávy

- Doména použitá pro odesílání pošty má zveřejněn TXT DNS záznam SPF, který má nastavenou výchozí politiku na soft fail (~all) nebo hard fail (-all).
- Minimálně hlavičky *From* a *Subject* a tělo zprávy odesílaných e-mailů jsou digitálně podepsány technologií DKIM, veřejný klíč použitý k podpisu je zveřejněn v DNS.
- Kryptografické prostředky použité pro podepsání zprávy dle DKIM jsou aktuálně odolné dle doporučení Úřadu.
- Doména použitá pro odesílání pošty má zveřejněn DMARC záznam v DNS.
- DMARC záznam má hodnotu parametru p nastaven na `quarantine` nebo `reject`.
- DMARC záznam nemá uveden parametr p nebo je hodnota parametru nastavena na 100.

- SMTP server při příjmu pošty kontroluje SPF, DKIM a DMARC přijaté zprávy. V případě, že některý z těchto údajů neodpovídá uvedené politice protistrany, e-mail je odmítnut, doručen do k tomu určené složky (Nevyžádaná pošta, spam apod.), nebo je pro uživatele viditelně označen jako potenciálně podvržený.

7 Další zdroje informací

Doporučovaným zdrojem informací k uvedeným technologiím jsou jednotlivé RFC, které jsou k nalezení na webu IETF (https://datatracker.ietf.org/).

Dalším zdrojem informací v českém jazyce jsou například následující články na webu Root.cz:

- https://www.root.cz/clanky/spf-proti-spamu-i-preposilani-posty/
- https://www.root.cz/clanky/dkim-podpisy-pro-duveryhodnejsi-e-mail/
- https://www.root.cz/clanky/dmarc-overeni-odesilatelovy-domeny/
- https://www.root.cz/clanky/protokol-dane-aneb-z-kroceni-zlych-certifikacnich-autorit/
- https://www.root.cz/clanky/mta-sts-bezpecne-dorucovani-posty-s-platnymi-tls-certifikaty/

Výzkumy týkající se zabezpečením e-mailové komunikace:

- https://www.usenix.org/conference/usenixsecurity20/presentation/lee-hyeonmin

8 Kam se mám obrátit v případě dotazů?

V souvislosti s ochranným opatřením se ve případě technických dotazů nebo dotazů na obsah jednotlivých uložených úkonů prosím obracejte na cert@nukib.cz. Na stejnou adresu nám prosím zašlete případné návrhy na vylepšení této metodiky. V případě mediálních dotazů se prosím obracejte na tiskového mluvčího Úřadu na dotazy.media@nukib.cz. V případě dalších dotazů, především právní povahy, týkajících se ochranného opatření se prosím obracejte na regulace@nukib.cz.

9 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
Zelená TLP: GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP: WHITE	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
11. října 2021	1.0	OVCERT	Vytvoření dokumentu