Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350 - 1117/2021
Číslo jednací:
8477/2021-NÚKIB-E/350

Brno, 11. října 2021

Vyřizuje:
Štěpán Daněk

VEŘEJNÁ VYHLÁŠKA

OPATŘENÍ OBECNÉ POVAHY

Národní úřad pro kybernetickou a informační bezpečnost se sídlem Brno, Mučednická 1125/31, PSČ 616 00 (dále jen „Úřad“) jako příslušný ústřední správní úřad podle § 22 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“),

stanovuje

na základě § 14 zákona o kybernetické bezpečnosti a postupem podle § 15 zákona o kybernetické bezpečnosti a § 171, § 173 a § 174 zákona č. 500/2004 Sb., správního řádu, ve znění pozdějších předpisů, **jako ochranné opatření tyto způsoby zvýšení ochrany informačních systémů, služeb a sítí elektronických komunikací:**

1. **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:**

   1.1. 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).

   1.2. V rámci zabezpečeného spojení všechny servery, přes které je přijímána nebo odesílána elektronická pošta:

      1.2.1. Podporují protokol TLSv1.2 nebo novější.

      1.2.2. Nepodporují protokol SSLv3 a starší.

1.2.3. 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.

1.2.4. 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.

1.3. Certifikáty všech SMTP serverů uvedených v MX záznamech jsou validní, vystaveny uznávanou certifikační autoritou a s doménovým názvem odpovídající názvu MX záznamu daného serveru.

1.4. 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.

1.5. 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.

1.6. Všechny používané MX záznamy SMTP serverů mají zveřejněn odpovídající TLSA záznam v DNS dle technologie DANE (IETF RFC 7672).

1.7. 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.

1.8. V případě komunikace mezi definovanými SMTP servery musí být tato komunikace zabezpečena aktuálně odolnými kryptografickými prostředky, dále musí být zajištěna nemožnost ponížení komunikace na nešifrovanou a obě strany musí zajistit ověřování autenticity protistrany. Použité kryptografické prostředky 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.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které jsou zároveň orgány veřejné moci zapojenými do předsednictví České republiky v Radě EU a které mají své zaměstnance evidované ke dni účinnosti tohoto opatření v Centrálním registru zaměstnanců podílejících se na přípravách a výkonu předsednictví v roce 2022, musí splnit body 1.1. až 1.5. nejpozději do 1. ledna 2022 a body 1.6. až 1.8. nejpozději do 1. července 2022.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které jsou zároveň orgány veřejné moci zapojenými do předsednictví České republiky v Radě EU, jejichž zaměstnanci budou do Centrálního registru zaměstnanců podílejících se na přípravách a výkonu předsednictví v roce 2022 zaevidováni po dni účinnosti tohoto opatření, musí splnit body 1.1. až 1.5. bez zbytečného odkladu po jejich zaevidování do tohoto registru, nejpozději však do 1. července 2022, a body 1.6. až 1.8. nejpozději do 1. července 2022.

Ostatní orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, musí splnit body 1.1. až 1.8. nejpozději do 1. ledna 2023.

Ostatní orgány a osoby, které se stanou povinnými osobami dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti po dni účinnosti tohoto ochranného opatření, musí body 1.1. až 1.8. splnit do 14 měsíců od svého určení či identifikace.

2. **Pokud přenos elektronické pošty z koncového zařízení probíhá na server elektronické pošty, který se nachází v odlišné síti než toto koncové zařízení, 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 tento přenos splňoval následující požadavky:**

   2.1. Využívá zabezpečené spojení pro všechny protokoly, kterými koncové zařízení komunikuje s poštovním serverem. Použité kryptografické prostředky v rámci zabezpečeného spojení 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.

   2.2. Pokud použitý přenos využívá pro zabezpečené spojení kryptografický protokol TLS, v rámci zabezpečeného spojení:

      2.2.1. Je využíván protokol TLSv1.2 nebo novější.

      2.2.2. Není využíván protokol SSLv3 a starší.

      2.2.3. Protokoly TLSv1.0 a TLSv1.1 mohou být povoleny v odůvodněných nezbytných případech, kdy by omezení podpory těchto protokolů mohlo způsobit omezení dostupnosti a řádného fungování systému elektronické pošty.

      2.2.4. Certifikát serveru elektronické pošty je validní a vystavený uznávanou certifikační autoritou. Pokud není certifikát vystaven uznávanou certifikační autoritou, použitá certifikační autorita musí být dostupná ve všech zařízeních, které se na poštovní server připojují.

   2.3. V případě využití protokolu SMTP (IETF RFC 5421) je využívána pouze zabezpečená variantu protokolu SMTPS.

   2.4. V případě využití protokolu IMAP (IETF RFC 9051) je využívána pouze zabezpečená variantu protokolu IMAPS.

2.5. V případě využití protokolu POP3 (IETF RFC 1939) je využívána pouze zabezpečená variantu protokolu POP3S.

2.6. V případě přístupu přes protokol HTTP nebo protokolu založeném na HTTP je využívána pouze zabezpečená varianta protokolu HTTPS.

2.7. V případě přístupu přes webové rozhraní musí být nastavena HTTP hlavička *Strict-Transport-Security* (HSTS, IETF RFC 6797) s hodnotou parametru *max-age* větším než nula.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které jsou orgány veřejné moci zapojenými do předsednictví České republiky v Radě EU a které mají své zaměstnance evidované ke dni účinnosti tohoto opatření nebo po tomto dni v Centrálním registru zaměstnanců podílejících se na přípravách a výkonu předsednictví v roce 2022, musí splnit body 2.1. až 2.7. nejpozději do 1. července 2022.

Ostatní orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, musí splnit body 2.1. až 2.7. nejpozději do 1. ledna 2023.

Ostatní orgány a osoby, které se stanou povinnými osobami dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti po dni účinnosti tohoto ochranného opatření musí body 2.1 až 2.7. splnit do 14 měsíců od svého určení či identifikace.

3. Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti zajistí, aby při přijímání a odesílání elektronické pošty protokolem SMTP mimo vnitřní síť byly splněny následující požadavky:

3.1. Domény použité pro odesílání elektronické pošty musí mít v DNS zveřejněn SPF záznam (IETF RFC 7208) obsahující adresy povolených SMTP serverů, které mohou odesílat elektronickou poštu. Výchozí politika musí být nastavena na *soft fail* (~all) nebo *hard fail* (-all).

3.2. Minimálně hlavičky *From* a *Subject* a tělo zprávy odesílané elektronické pošty musí být digitálně podepsány technologií DKIM (IETF RFC 6376), veřejná část klíče musí být zveřejněna v DNS. Kryptografické prostředky použité pro podepsání zprávy musí být aktuálně odolné dle doporučení Úřadu pro kryptografické prostředky vydávaného v návaznosti na § 26 písm. d) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, jiné prostředky mohou být použity pouze v odůvodněných případech.

3.3. Domény použité pro odesílání elektronické pošty musí mít v DNS zveřejněn DMARC záznam (IETF RFC 7489) minimálně s těmito parametry:

3.3.1. *Requested Mail Receiver policy* (p) nastaveným na *quarantine* nebo *reject* a

3.3.2. *Sampling rate* (pct) nastaven na 100 (výchozí hodnota).

3.4. Při příjmu elektronické pošty je ověřováno, zda adresa serveru, ze kterého byla pošta odeslána, souhlasí s SPF záznamem domény, pokud je SPF záznam protistranou

zveřejněn. V případě, že těmto pravidlům nevyhovuje, je poštovní zpráva odmítnuta, zahozena, doručena do k tomu určené složky, nebo zřetelně označena jako pravděpodobně podvržená.

3.5. Při příjmu elektronické pošty je ověřován digitální podpis hlaviček a těla poštovní zprávy technologií DKIM, pokud byly hlavičky a tělo zprávy touto technologií podepsány.

3.6. Při příjmu elektronické pošty je kontrolováno, zda poštovní zpráva vyhovuje pravidlům uvedeným v DMARC záznamu protistrany, pokud jej protistrana zveřejnila. V případě, že těmto pravidlům nevyhovuje, je poštovní zpráva odmítnuta, zahozena, doručena do k tomu určené složky, nebo zřetelně označena jako pravděpodobně podvržená.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které jsou orgány veřejné moci zapojenými do předsednictví České republiky v Radě EU a které mají své zaměstnance evidované ke dni účinnosti tohoto opatření v Centrálním registru zaměstnanců podílejících se na přípravách a výkonu předsednictví v roce 2022, musí splnit bod 3.1. do 1. ledna 2022 a body 3.2. až 3.6. nejpozději do 1. července 2022.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které jsou orgány veřejné moci zapojenými do předsednictví České republiky v Radě EU a které budou mít své zaměstnance zaevidované do Centrálního registru zaměstnanců podílejících se na přípravách a výkonu předsednictví v roce 2022 po dni účinnosti tohoto opatření, musí splnit bod 3.1. bez zbytečného odkladu po jejich zaevidování do tohoto registru, nejpozději však do 1. července 2022, a body 3.2. až 3.6. nejpozději do 1. července 2022.

Ostatní orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, musí splnit body 3.1. až 3.6. nejpozději do 1. ledna 2023.

Ostatní orgány a osoby, které se stanou povinnými osobami dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti po dni účinnosti tohoto ochranného opatření, u nichž je toto ochranné opatření relevantní, musí body 3.1. až 3.6. splnit do 14 měsíců od svého určení či identifikace.

Toto ochranné opatření je nutno provést ve lhůtách k tomu určených u jednotlivých úkonů.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které některé výše uvedené úkony provedly, nemusí tyto konkrétní úkony provádět opakovaně.

ODŮVODNĚNÍ

1. Národní úřad pro kybernetickou a informační bezpečnost jako ústřední orgán státní správy podle § 2 bodu 16 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, a podle § 22 písm. b) zákona o kybernetické bezpečnosti, dospěl v souladu s § 14 zákona o kybernetické bezpečnosti na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu k vydání tohoto opatření obecné povahy za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací, tak jak jsou uvedeny ve výroku tohoto opatření obecné povahy. K vydání tohoto opatření obecné povahy dochází na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu ze dne 20. února 2020, který byl zaevidován pod číslem 32305.

2. Incident byl způsoben útokem typu *Man-in-the-Middle* (MITM) na prvek mimo infrastrukturu organizace povinné osoby, kdy se útočník dostal do pozice prostředníka mezi komunikujícími subjekty, čímž byla narušena důvěrnost přenášených elektronických poštovních zpráv přenášených skrz tento prvek.

3. Jednotlivé způsoby zvýšení ochrany informačních systémů, služeb a sítí elektronických komunikací, jak jsou specifikovány ve výroku tohoto opatření obecné povahy, jsou v obecné rovině úkony, jejichž provedení je nezbytné k zajištění důvěrnosti a integrity komunikace mezi poštovními servery povinných osob a mezi koncovými zařízeními a poštovním serverem v rámci organizace povinné osoby. Dále pak tyto způsoby zvýšení ochrany směřují k zamezení podvržení e-mailové komunikace (např. zasílání zpráv s podvrženou doménou organizace). V případě nezavedení těchto způsobů zvýšení ochrany hrozí možnost narušení důvěrnosti a integrity zasílané elektronické komunikace, což může mít vážné přímé dopady na fungování a důvěryhodnost dotčených organizací. V případě orgánů veřejné moci spolupracujících na činnostech v rámci předsednictví České republiky v Radě EU by narušením bezpečnosti vzájemné komunikace mohlo dojít k narušení řádného průběhu tohoto předsednictví a snížení důvěryhodnosti České republiky na mezinárodním poli.

4. Zavedení výše uvedených způsobů zvýšení ochrany informačních systémů je nezbytně nutné pro zajištění bezpečné komunikace zejména mezi orgány veřejné moci navzájem, interně v rámci těchto orgánů veřejné moci, případně také mezi orgány veřejné moci a dalšími povinnými osobami. Má-li některé z požadovaných způsobů zvýšení ochrany zavedeny pouze jeden z komunikujících subjektů, probíhá celá komunikace v neadekvátně zabezpečené (nešifrované) podobě nebo je náchylná na útoky typu MITM a navržené způsoby zvýšení ochrany tak postrádají smysl, pročež je nezbytné, aby došlo k jejich implementaci co nejširší množinou povinných subjektů dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti. V opačném případě může běžně docházet k opakovaným

incidentům srovnatelným s těmi, jejichž analýza vedla k vydání tohoto ochranného opatření.

5. Bližší technické odůvodnění a vysvětlení nezbytnosti konkrétních způsobů zabezpečení informačních systémů nebo služeb a sítí elektronických komunikací povinných subjektů je obsaženo v části „Technické odůvodnění“.

6. Na základě § 14 zákona o kybernetické bezpečnosti jsou výše uvedenými způsoby zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací vázáni všichni správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby.

7. Povinné osoby dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti musí výše popsané způsoby zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací implementovat za předpokladu, že je jejich systém elektronické pošty součástí systému řízení bezpečnosti informací, který se vztahuje k systémům, na které musí být uplatňovány požadavky zákona o kybernetické bezpečnosti. Konkrétně u správců a provozovatelů informačních systémů základní služby tomu tak bude vždy za předpokladu, že je fungování základní služby závislé mimo jiné také na systému elektronické pošty. U správců a provozovatelů informačních a komunikačních systémů kritické informační infrastruktury tomu tak bude vždy za předpokladu, že bude systém elektronické pošty součástí určeného prvku kritické informační infrastruktury. U správců a provozovatelů významných informačních systémů, kteří jsou organizační složkou státu, krajem nebo hlavním městem Praha, je systém elektronické pošty typovým významným informačním systémem dle § 2 odst. 1 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů (dále jen „vyhláška o VIS“), tudíž bude implementaci způsobů zvýšení ochrany nutné provést vždy. U ostatních orgánů veřejné moci tomu tak bude za předpokladu, že jejich systém elektronické pošty naplňuje určující kritéria dle § 3 vyhlášky o VIS. Nadto mohou všechny povinné osoby dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti implementaci provést na základě toho, že svůj systém elektronické pošty zařadily do rozsahu systému řízení bezpečnosti informací.

8. Na základě § 14 zákona o kybernetické bezpečnosti je k provedení způsobů zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací nutno stanovit přiměřenou lhůtu. S ohledem na výše uvedené způsoby zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací a odůvodnění těchto způsobů v rámci Technického odůvodnění považuje Úřad lhůty stanovené ve výroku tohoto opatření obecné povahy za dostatečné a přiměřené. To platí jak ve vztahu k osobám uvedeným v § 3 písm. c) až f) zákona o kybernetické bezpečnosti k datu účinnosti tohoto opatření, tak ve vztahu k osobám a orgánům, které se povinnými

osobami uvedenými v § 3 písm. c) až f) zákona o kybernetické bezpečnosti stanou v budoucnosti.

9. Kratší lhůta pro orgány veřejné moci podílející se na předsednictví České republiky v Radě EU vyplývá z časového rámce tohoto předsednictví. Některé agendy se začínají řešit v zásadě již od začátku roku 2022, přičemž Česká republika Radě EU fakticky předsedá od července 2022 do konce roku 2022. Je tedy nezbytné zajistit, aby byly způsoby zvýšení ochrany implementovány právě ve lhůtách odpovídajících tomuto časovému rámci, tedy ideálně již od 1. ledna 2022 a nejpozději právě k 1. červenci 2022.

10. Přechodná ustanovení dle § 30 a § 31 zákona o kybernetické bezpečnosti a čl. II přechodných ustanovení zavedených zákonem č. 205/2017 Sb., které dávají povinným osobám dle § 3 písm. c) až f) tohoto zákona 1 rok od jejich určení či identifikace na zavedení bezpečnostních opatření se nevztahují na plnění povinností uložených tímto opatřením.

11. Úřad upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti, při hodnocení rizik a v plánu zvládání rizik zohlední opatření podle § 11 zákona o kybernetické bezpečnosti. Jedním z těchto opatření je i ochranné opatření podle § 14 zákona o kybernetické bezpečnosti.

12. Úřad dále upozorňuje, že v souladu s § 4 odst. 4 zákona o kybernetické bezpečnosti jsou orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle zákona o kybernetické bezpečnosti nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

13. S ohledem na stanovené lhůty si Úřad dovoluje upozornit na ustanovení § 29 písm. c) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, dle kterého *„zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení, jde-li o zadávání nebo plnění veřejné zakázky v rámci zvláštních bezpečnostních opatření stanovenými jinými právními předpisy a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo.“* Je na zvážení povinné osoby v pozici zadavatele implementujícího shora uvedené způsoby zvýšení ochrany, zda je institut této výjimky s ohledem na specifické okolnosti a podmínky dané organizace použitelný a aplikovatelný.

Technické odůvodnění

Opatření pro zajištění důvěrnosti a integrity komunikace mezi poštovními servery

14. První část výroku opatření směřuje k zajištění důvěrnosti a integrity komunikace mezi poštovními servery, které se nachází mimo vnitřní síť a míří na snížení možnosti provádět útoky typu MITM.

15. Šifrování je základní způsob zajištění důvěrnosti a integrity komunikace tak, aby její obsah nemohl číst nebo upravovat útočník mající přístup ke komunikaci mezi poštovními servery.

16. Pro přenos elektronických poštovních zpráv mezi servery se využívá protokol SMTP, který v základní verzi nepodporuje šifrování. Rozšíření protokolu SMTP, STARTTLS (IETF RFC 3207), umožňuje tzv. oportunistické šifrování (tedy takové, které se použije, pokud to lze; jinak dojde k přepnutí na nešifrovanou komunikaci). Server nejprve naváže nešifrované spojení, které je následně povýšeno na šifrované. Pro povýšení spojení na šifrované musí toto rozšíření podporovat jak strana odesílatele, tak strana příjemce. Rozšíření STARTTLS samo o sobě chrání pouze proti pasivnímu odposlechu přenášených zpráv. Zavedení podpory tohoto rozšíření je obsahem bodu 1.1 výroku tohoto opatření.

17. V rámci zabezpečeného spojení je pro zajištění důvěrnosti a integrity nutné využít pouze aktuálně odolné kryptografické prostředky. Ty definuje Úřad v rámci doporučení zveřejněných na webových stránkách úřadu. Dále je vyžadována podpora určitých verzí kryptografických protokolů určených pro navazování zabezpečeného spojení. Protokol SSLv3 byl označen jako zastaralý v roce 2015 (IETF RFC 7568). Protokoly TLSv1.0 a TLSv1.1 byly označeny jako zastaralé v roce 2021 (IETF RFC 8996). V současné době je tak doporučováno využívat TLSv1.2 (IETF RFC 5246) a TLSv1.3 (IETF RFC 8446). Zastaralé protokoly jsou náchylné na různé typy útoků, které mohou vést k narušení důvěrnosti a integrity komunikace. Využívání aktuálně odolných kryptografických prostředků a omezení podpory zmíněných zastaralých verzí protokolů jak při příjmu, tak odesílání pošty, vyžaduje bod 1.2 výroku tohoto opatření.

18. Pro ověření protistrany jsou v rámci protokolu TLS využívány certifikáty. Pro ověření certifikátu musí být certifikát platný a vystavený uznávanou certifikační autoritou. Seznam obecně uznávaných certifikačních autorit je zveřejňován v rámci Common CA Database (https://www.ccadb.org), kde certifikát certifikační autority musí být zařazen jak v seznamu společnosti Mozilla, tak společnosti Microsoft. Povinnost využívání platného a uznávaného certifikátu je zakotvena v bodě 1.3 výroku tohoto opatření.

19. Pro zjišťování, na jakou IP adresu SMTP serveru má být elektronická poštovní zpráva poslána, je používán protokol DNS, který nezajišťuje integritu DNS záznamů. Pro zajištění integrity DNS zpráv je využíváno rozšíření DNSSEC (IETF RFC 4033). Všechny DNS záznamy

relevantní pro příjem pošty (tedy minimálně MX záznamy u domény určené pro příjem pošty, a následně A popř. AAAA záznamy u doménových názvů SMTP serverů), musí být digitálně podepsány touto technologií, což je obsahem bodu 1.4 výroku tohoto opatření.

20. Při odesílání elektronické pošty musí být digitální podpisy DNS záznamů validovány, k čemuž musí být využit DNS server podporující validaci dle technologie DNSSEC nebo musí validaci provádět přímo SMTP server. Pokud validaci provádí SMTP server, komunikace mezi SMTP a DNS serverem musí být zabezpečena tak, aby ji případný útočník neměl možnost podvrhovat. K tomu je nutné, aby se DNS server nacházel buď na stejném serveru (virtuálním nebo fyzickém), ve stejné síti nebo komunikace byla zabezpečena před narušením integrity kryptografickými algoritmy jiným způsobem (např. v rámci VPN spojení, DNS-over-HTTPS nebo DNS-over-TLS). V případě, že je využíváno více DNS serverů, musí validaci provádět všechny použité servery. Zavedení validace DNSSEC vyplývá z bodu 1.5 výroku tohoto opatření.

21. Vzhledem k oportunistické povaze šifrování u protokolu STARTTLS (viz výše bod 16) je při navazování spojení možné v případě aktivního útoku typu Man-in-the-Middle (MITM), kdy se útočník dostane do pozice prostředníka mezi komunikujícími subjekty, přerušit navazování šifrovaného spojení (*STRIPTLS*), v takovém případě je pak komunikace nešifrovaná. Nešifrovaný přenos umožňuje narušit důvěrnost a integritu přenášené zprávy, neboť útočník může zprávu číst nebo i upravovat. Taktéž vzhledem k výchozímu nastavení SMTP serverů, kdy nedochází ke kontrole certifikátu při navazování spojení, je možné provádět útok typu *TLS Certificate Spoofing*. Pro zabránění tomuto typu útoku byly vytvořeny dvě komplementární technologie – DANE (IETF RFC 7671) a MTA-STS (IETF RFC 8461). K efektivnímu zabezpečení přenášených zpráv musí jednu z těchto technologii podporovat jak strana odesílatele, tak strana příjemce, přičemž je nezbytné, aby oba komunikující subjekty využívaly stejný druh technologie, tj. buď DANE, nebo MTA-STS. Z důvodu maximálního možného efektu tohoto ochranného opatření uložil Úřad implementaci technologie DANE, pro zajištění kompatibilní zabezpečené komunikace mezi co nejširším okruhem povinných subjektů.

22. 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 předaného při navazování TLS spojení. V případě, že vzdálený server neoznámí podporu zabezpečeného spojení (např. v důsledku útoku *STRIPTLS*) či nesouhlasí otisk certifikátu, komunikace nebude navázána, a tudíž poštovní zpráva nebude odeslána. Zavedení technologie DANE nevylučuje souběžné využití technologie MTA-STS.

23. Pro správnou funkci DANE musí být pro zabezpečení komunikace přijímání elektronické poštovní zprávy zveřejněn TLSA záznam v DNS. Ten obsahuje otisk certifikátu, který je použit při příjmu elektronické pošty. Protistrana tak má možnost zkontrolovat, zda server

podporuje zabezpečenou komunikaci pomocí STARTTLS a nabídnutý certifikát nebyl podvržen nezávislým kanálem. Pokud by se tak stalo, elektronická poštovní zpráva nebude na tento server odeslána a bude tak ochráněna před narušením důvěrnosti a integrity. Pro zajištění integrity TLSA záznamu a aby mohla protistrana tomuto záznamu důvěřovat, musí být tento záznam podepsán technologií DNSSEC. Zveřejnění tohoto záznamu vyžaduje bod 1.6 výroku tohoto opatření a digitální podpis dle DNSSEC bod 1.4 opatření.

24. Pro zabezpečení komunikace při odesílání elektronické poštovní zprávy musí být TLSA záznam u protistrany kontrolován, pokud je tento záznam zveřejněn. Pokud se nepodaří navázat zabezpečené spojení nebo otisk certifikátu neodpovídá, elektronická poštovní zpráva na tento server nesmí být odeslána. Kontrolu tohoto záznamu vyžaduje bod 1.7 výroku tohoto opatření.

25. Poslední bod výroku opatření se zabývá situací, kdy je elektronická pošta přeposílána mezi poštovními servery mimo vnitřní síť, např. v případě využití služby třetí strany pro kontrolu přijímané a odesílané pošty. V takovém případě je nutné pro zamezení útoku typu MITM zajistit, aby tato komunikace byla zabezpečena kryptografickými prostředky, nebylo možné tuto komunikaci ponížit na nešifrovanou a zároveň je třeba ověřovat autenticitu protistrany. Zpravidla se tedy bude jednat o využití protokolu SMTPS, může být ale zvoleno i jiné technické řešení, které zajistí tyto požadavky (např. SMTP komunikace v rámci VPN spojení).

26. Vzhledem k tomu, že body 1.1 až 1.5 výroku opatření jsou dle interního průzkumu Úřadu relevantními orgány veřejné moci většinově implementovány, je k jejich zavedení stanovena kratší lhůta. Zavedení ostatních bodů může znamenat implementaci nových technologií, a proto je lhůta pro jejich zavedení delší.

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

27. Druhá část výroku opatření směřuje k zabezpečení komunikace mezi koncovým zařízením (např. koncová stanice nebo mobilní zařízení) a serverem elektronické pošty, tak aby byla snížena možnost provádět útoky typu MITM. Opatření je potřeba zavádět pouze v případě, že se koncové zařízení nachází v jiné síti, než server elektronické pošty (typicky tedy v případě, kdy komunikace mezi koncovým zařízením a serverem probíhá přes Internet).

28. Šifrování je základní způsob zajištění důvěrnosti a integrity přenášených zpráv, tak aby jejich obsah nemohl číst nebo upravovat útočník mající přístup ke komunikaci mezi koncovým zařízením a poštovním serverem.

29. Pro fungující šifrování se musí používat pouze aktuálně odolné kryptografické algoritmy, které definuje Doporučení v oblasti kryptografických prostředků dostupné na webových stránkách Úřadu. V bodu 2.1 výroku tohoto opatření jak tak zakotvena povinnost povinného subjektu používat zabezpečené spojení za pomoci využití kryptografických prostředků uvedených ve zmiňovaném Doporučení.

30. V případě, že použitý protokol využívá kryptografický protokol TLS, specifikuje bod 2.2 výroku opatření, které verze tohoto protokolu je možné použít.

31. Pro ověření protistrany jsou v rámci protokolu TLS využívány certifikáty. Pro ověření certifikátu musí být certifikát platný a vystavený uznávanou certifikační autoritou. Seznam obecně uznávaných certifikačních autorit je zveřejňován na Common CA Database, kde certifikát certifikační autority musí být zařazen jak v seznamu společnosti Mozilla, tak společnosti Microsoft. Použití jiné certifikační autority, která není zveřejněna v seznamu CCAD, je možné, pokud je akceptována všemi koncovými zařízeními, které přistupují k poštovnímu serveru. Povinnost využívání platného a uznávaného certifikátu je zakotvena v bodě 2.2.4. výroku tohoto opatření.

32. U protokolů SMTP, IMAP, POP3 nebo HTTP (včetně protokolů založených na HTTP) se v bodech 2.3 až 2.6 výroku opatření vyžaduje používání zabezpečených verzí těchto protokolů (SMTPS, IMAPS, POP3S, HTTPS), které nejsou náchylné na ponížení spojení na nešifrované.

33. V souvislosti s využíváním protokolu HTTPS při přístupu přes webové rozhraní je v bodu 2.7 výroku opatření povinnost nastavení HTTP hlavičky *Strict-Transport-Security* dle ITFC RFC 6797. Hodnota parametru *max-age* musí být větší než nula, aby prohlížeče tuto hlavičku akceptovaly. Toto opatření brání ponížení spojení na nešifrované spojení HTTP.

Opatření pro zajištění integrity a zamezení podvržení odesilatele elektronické poštovní zprávy

34. Třetí část výroku opatření se zaměřuje zajištění integrity přenášených zpráv elektronické pošty. Tato opatření umožní detekovat pozměnění zprávy útočníkem, pokud strana odesilatele nebo příjemce nepodporuje opatření z první části výroku. Zároveň zamezí podvržení odesilatele poštovních zpráv. Podvržení odesilatele je využíváno útočníky pro zvýšení důvěryhodnosti phishingových zpráv.

35. Body 3.1 až 3.3 výroku opatření směřují k zabezpečení toho, aby bylo možné detekovat narušení integrity elektronické poštovní zprávy při odesílání. Zároveň zabezpečují, aby útočník nemohl posílat elektronickou poštovní zprávu s podvrženou doménou organizace.

36. Body 3.4 až 3.6 výroku opatření směřují k zabezpečení toho, aby bylo možné detekovat narušení integrity elektronické poštovní zprávy při příjmu. Zároveň zabezpečují, aby

podvržené elektronické poštovní zprávy nebyly doručeny do schránek uživatelů organizace nebo byl uživatel na možné podvržení zprávy upozorněn.

37. Technologie SPF (Sender Policy Framework) umožňuje organizaci definovat, které SMTP servery mohou posílat elektronické poštovní zprávy z domény organizace. Výchozí politika *soft* nebo *hard fail* definuje, jak má vzdálený poštovní server naložit se zprávou, pokud je odeslána z jiných než definovaných serverů.

38. Technologie DKIM (DomainKeys Identified Mail) digitálně podepisuje určené hlavičky a tělo poštovní zprávy, a tak protistraně zaručuje, že poštovní zpráva byla odeslána z legitimního SMTP serveru. Podepisující privátní klíč je uložen na SMTP serverech zasílajících poštovní zprávu, veřejný klíč pro ověření podpisu je zveřejněn v TXT záznamu v rámci DNS záznamu domény.

39. 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. Pro zabránění doručení zprávy s narušenou integritou nebo potenciálně podvržené zprávy přímo uživateli musí být politika nastavena na *quarantine* nebo *reject*. Dále se vyžaduje nastavení hodnoty parametru *Sampling rate* na 100, tak aby se tato politika uplatnila na všechny odeslané zprávy. Samotné použití technologie SPF není dostatečné, neboť ta kontroluje pouze adresu *envelope-from*, přičemž příjemci zprávy se typicky zobrazuje adresa odesilatele uvedená v hlavičce *From*.

40. Bod 3.1 výroku opatření je dle interního průzkumu Úřadu napříč orgány veřejné moci již většinově splněn a jeho zavedení je snadnější, proto je lhůta na jeho zavedení relevantními orgány veřejné moci kratší. Ostatní body opatření mohou znamenat implementaci nových technologií, proto je lhůta na jejich zavedení delší.

41. Je nutné zdůraznit, že ani všechna uvedená opatřeních nenahrazují zabezpečení elektronických poštovních zpráv pomocí end-to-end šifrování (např. PGP, S/MIME), pouze zvyšují zabezpečení komunikace mezi jednotlivými prvky umožňující přenos elektronické pošty.

42. V souvislosti s tímto ochranným opatřením se v případě technických dotazů nebo dotazů na obsah jednotlivých uložených úkonů prosím obracejte na cert@nukib.cz. 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.

POUČENÍ

Toto opatření obecné povahy se doručuje postupem podle § 25 správního řádu veřejnou vyhláškou na úřední desce Úřadu. Opatření obecné povahy podle § 14 zákona o kybernetické

bezpečnosti nabývá na základě § 15 odst. 1 zákona o kybernetické bezpečnosti účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu. Ustanovení § 172 správního řádu se nepoužije. Na základě § 15 odst. 2 zákona o kybernetické bezpečnosti lze k opatření obecné povahy vydanému podle § 14 uplatnit připomínky, a to ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.

Digitálně podepsal:
Ing. Karel Řehka
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 11.10.2021 09:23

NÚKIB

Ing. Karel Řehka
ředitel
elektronicky podepsáno

Vyvěšeno dne: .....

Sejmuto dne: .....