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

OCHRANNÉ OPATŘENÍ K ZABEZPEČENÍ E-MAILŮ ZE DNE 11. 10. 2021

Často kladené otázky

1 Úvod

Tento dokument poskytuje stručné odpovědi na nejčastější otázky týkající se 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 (dále jen „zákon o kybernetické bezpečnosti“), 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.

S technickými dotazy nebo dotazy na obsah jednotlivých uložených úkonů prosím obracejte na cert@nukib.cz.

S mediálními dotazy se prosím obracejte na tiskového mluvčího Úřadu na komunikace@nukib.cz.

Jakékoli další dotazy, především právní povahy, prosím směřujte na regulace@nukib.cz.

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

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 Často kladené otázky

2.1 Na koho ochranné opatření dopadá?

Ochranné opatření dopadá na všechny povinné osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, jejichž elektronická pošta je součástí informačního systému, na který se vztahují požadavky zákona o kybernetické bezpečnosti. Konkrétně jde o:

- **správce a provozovatele informačních nebo komunikačních systémů kritické informační infrastruktury**, u nichž je systém elektronické pošty součástí určeného prvku kritické informační infrastruktury;
- **správce a provozovatele významných informačních systémů**, tedy
  - organizační složky státu a kraje včetně hl. m. Prahy, u nichž 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“),
  - ostatní orgány veřejné moci, jejichž systém elektronické pošty naplňuje určující kritéria dle § 3 vyhlášky o VIS;
- **správce a provozovatele informačního systému základní služby**, za předpokladu, že je fungování základní služby závislé mimo jiné také na systému elektronické pošty.

2.2 Jak se opatření dotkne běžných uživatelů a organizací nespadajících pod zákon o kybernetické bezpečnosti?

E-mailové zprávy od běžných uživatelů budou i nadále schopné doputovat orgánům veřejné moci, takže na straně běžných uživatelů není třeba dělat žádné změny. Občanům a soukromým společnostem nehrozí žádné omezení běžné komunikace s úřady.

Dobrovolné zavedení technologií a postupů popsaných v opatření každopádně doporučujeme také organizacím, které nespadají pod zákon o kybernetické bezpečnosti. Používáním doporučených technologií mohou zásadním způsobem zvýšit zabezpečení své elektronické pošty.

2.3 Znamená to tedy, že aktuálně není bezpečnost e-mailové komunikace zajištěna nijak?

Kybernetická bezpečnost není jako vypínač, který je buď zapnutý, nebo vypnutý. Vždy se budeme bavit o určité úrovni kybernetické bezpečnosti. Aktuální úroveň bezpečnosti e-mailové komunikace jsme vzhledem k významu komunikace orgánů veřejné moci, zvláště s ohledem na nadcházející předsednictví v Radě EU, a dalších subjektů vyhodnotili jako nedostatečnou, a proto iniciujeme její zvýšení.

Úřad opatření vydává na základě zkušeností z řešení dříve mu nahlášených incidentů, aby došlo ke zvýšení standardu zabezpečení komunikace napříč povinnými osobami. Nejedná se o reakci na jakoukoli bezprostřední či konkrétní hrozbu.

2.4 Od kdy a do kdy je ochranné opatření účinné?

Ochranné opatření je účinné dnem jeho vyvěšení na úřední desce Úřadu, tedy od **11. října 2021**.

Ochranné opatření **zůstává účinné do budoucna** do doby, kdy ho úřad zruší nebo jej nenahradí novým opatřením.

Opatření se vztahuje také na subjekty, které se povinnými osobami dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti stanou až po 11. říjnu 2021.

2.5 Do kdy je třeba zavést způsoby zvýšení ochrany obsažené v ochranném opatření?

Orgány veřejné moci zapojené do předsednictví České republiky v Radě EU, 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. a bod 3.1.** výroku ochranného opatření nejpozději do **1. ledna 2022**,
- body **1.6. až 1.8., 2.1 až 2.7. a 3.2. až 3.6.** výroku ochranného opatření nejpozději do **1. července 2022**.

Orgány veřejné moci zapojené do předsednictví České republiky v Radě EU, které budou mít své zaměstnance zaevidované v Centrálním registru zaměstnanců podílejících se na přípravách a výkonu předsednictví v roce 2022 až po dni účinnosti tohoto opatření musí splnit:

- body **1.1. až 1.5. a bod 3.1.** výroku ochranného opatření bez zbytečného odkladu po jejich zaevidování do tohoto registru, nejpozději však **1. července 2022**,
- body **1.6. až 1.8., 2.1. až 2.7. a 3.2. až 3.6.** výroku ochranného opatření nejpozději do **1. července 2022.**

Ostatní orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti musí splnit:

- **všechny body** výroku ochranného opatření 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 splnit:

- **všechny body** výroku ochranného opatření nejpozději **do 14 měsíců od svého určení či identifikace**.

2.6 Co je účelem ochranného opatření?

Způsoby zvýšení ochrany informačních systémů, služeb a sítí elektronických komunikací obsažené v ochranném opatření 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. Kromě zabezpečení komunikace mezi povinnými osobami bude taktéž zvýšena ochrana komunikace mezi veřejností a orgány veřejné moci. Dále pak tyto způsoby zvýšení ochrany směřují k **zamezení podvržení e-mailové komunikace** (např. zasílání zpráv s podvrženou doménou organizace).

Specificky 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.

2.7 Jaká je právní povaha ochranného opatření?

Ochranné opatření je vydáno na základě ustanovení § 14 a § 15 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu.

Právní formou ochranného opatření je **opatření obecné povahy** dle § 171 a násl. zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů. V případě ochranného opatření se však neuplatní § 172 správního řádu, což vyplývá z § 15 zákona o kybernetické bezpečnosti. Tedy ochranné opatření je účinné okamžikem vyvěšení.

2.8 Jak mám zavést požadované způsoby zvýšení ochrany?

Ke správnému zavedení veškerý způsobů zvýšení ochrany slouží podpůrný materiál *Metodika k zavedení způsobů zvýšení ochrany dle ochranného opatření ze dne 11. 10. 2021*, který je dostupný na webových stránkách Úřadu.

2.9 Za jakých podmínek lze pro zabezpečení e-mailu využít služby cloud computingu ?

Povinné osoby, které nejsou orgány veřejné moci, nemají stanoveny žádné zvláštní podmínky pro využití služeb cloud computingu nad rámec zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti (zejm. ustanovení o řízení dodavatelů).

Podmínky využití služeb cloud computingu orgány veřejné moci upravuje § 4 odst. 5 ZKB a Hlava VI. zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS).

Orgány veřejné moci musí při využití služby cloud computingu v rámci informačního systémů využívaného pro výkon veřejné moci zařadit tento informační systém nebo jeho část (bezpečnostní komponentu) do bezpečnostní úrovně dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. Bezpečnostní pravidla pro využívání cloud computingu orgány veřejné moci zatím nebyly vydány, není tak možné, a tedy ani nutné, je zohlednit.

Je-li e-mailové řešení zároveň informačním systémem veřejné správy dle ZoISVS je obecně třeba vybírat službu cloud computingu zapsanou v katalogu cloud computingu. To neplatí, pokud služba cloud computingu slouží výlučně ke správě a řešení technických potíží nebo diagnostice

programových anebo technických prostředků, případně k **zabezpečení** nebo přenosu s tím souvisejících signálů (viz § 6l odst. 4 písm. a ZoISVS). V případě, že bude službou cloud computingu pouze bezpečnostní komponenta, lze uvažovat o aplikaci této výjimky. Gestorem ZoISVS je však Ministerstvo vnitra, které je proto povoláno k výkladu a aplikaci dané výjimky.

Dle přechodných ustanovení v čl. LXXXI, odst. 4 zákona č. 261/2021 Sb. (tzv. DEPO) platí, že orgán veřejné správy může využívat cloud computing, jehož využívání započalo v době mezi 1. zářím 2021 a 31. lednem 2022, až do 31. prosince 2022, aniž je splněna podmínka nákupu této služby skrze katalog cloud computingu.

2.10 Může v důsledku implementace opatření dojít k omezení komunikace?

Zavedení způsobů zvýšení ochrany nemůže omezit doručování e-mailových zpráv ze strany veřejnosti, případně interně v rámci organizace. V případě řádné implementace ochranného opatření tak povinným osobám nehrozí žádné omezení odesílání a doručování elektronické pošty, ať už interně nebo externě.

2.11 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. V případě mediálních dotazů se prosím obracejte na tiskového mluvčího Úřadu na komunikace@nukib.cz. V případě dalších dotazů, především právní povahy, týkajících se ochranného opatření se prosím obracejte na regulace@nukib.cz.

3 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**
8. října 2021	1.0	OREVES	Vytvoření dokumentu