Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

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

Spisová značka:
350 - 409/2021
Číslo jednací:
2377/2021-NÚKIB-E/350

Brno, 11. března 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,

stanovuje

na základě § 13 odst. 3 zákona o kybernetické bezpečnosti a postupem podle § 15 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon 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 v souvislosti se zranitelnostmi Microsoft Exchange Server označenými jako CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 a CVE-2021-26858.**

Úkony uložené tímto reaktivním opatřením se vztahují na Microsoft Exchange Server 2010, 2013, 2016 a 2019, které měly přístupný Outlook Web Access (OWA) do veřejné sítě Internet v období od 1. prosince 2020 do vydání tohoto reaktivního opatření, s výjimkou těch, které byly nebo jsou provozovány jako služba Microsoft 365 nebo Exchange online. (dále jen „Microsoft Exchange Server“)

Reaktivní opatření jsou povinny provést všechny orgány a osoby podle § 3 písm. c) až f) zákona o kybernetické bezpečnosti, s výjimkou těch případů Microsoft Exchange Server, u kterých orgán nebo osoba v období od 3. března 2021 do vydání tohoto reaktivního opatření nahlásily Úřadu postupem podle § 8 odst. 1 zákona o kybernetické bezpečnosti kybernetický bezpečnostní incident týkající se využití zranitelnosti Microsoft Exchange Server.

Reaktivní opatření se skládá z následujících úkonů, které jsou orgány a osoby povinny provést ve stanovené lhůtě:

1) Neprodleně identifikujte, zda je Microsoft Exchange Server součástí informačního systému nebo sítě elektronických komunikací regulovaného zákonem o kybernetické bezpečnosti, zda je Microsoft Exchange Server součástí stanoveného rozsahu systému řízení bezpečnosti informací, nebo zda používáte Microsoft Exchange Server, který sice není součástí systému nebo sítě elektronických komunikací regulovaného zákonem o kybernetické bezpečnosti nebo rozsahu systému řízení bezpečnosti informací, avšak v rámci orgánu nebo osoby může jinak ohrozit informační systém nebo síť elektronických komunikací, které jsou regulované zákonem o kybernetické bezpečnosti.

2) V případě, že v souladu s bodem 1) identifikujete Microsoft Exchange Server,

    a) zašlete neprodleně Úřadu rozsah veřejných DNS záznamů nebo veřejných IP adres využívaných Microsoft Exchange Server podle bodu 1),

    b) použijte v rámci Microsoft Exchange Server nástroj označený jako „Test-ProxyLogon.ps1“ a neprodleně informujte Úřad o pozitivních i negativních nálezech tohoto nástroje,

    c) prověřte za období od 1. prosince 2020 do vydání tohoto reaktivního opatření níže uvedené síťové indikátory kompromitace, a neprodleně informujte Úřad o pozitivních i negativních nálezech,

    d) vyhledejte nelegitimně nahrané nebo upravené soubory (zejména ASPX, PHP, JS) v souborovém systému Microsoft Exchange Server. V případě pozitivního nálezu zajistěte vzorek souboru, přesný čas vytvoření souboru a umístění souboru. Takto zajištěné informace neprodleně zašlete Úřadu,

    e) v případě pozitivních nálezů v úkonu podle písm. d) zajistěte z Microsoft Exchange Server ECP logy, HTTP logy, Windows Event logy a export registrových klíčů. Takto zajištěné informace neprodleně zašlete Úřadu. Zaslání výše uvedených logů a klíčů lze nahradit zasláním forenzního obrazu disku a paměti Microsoft Exchange Server,

    f) v případě pozitivních nálezů v úkonu podle písm. d) zajistěte síťové logy související s pozitivními nálezy. Tyto síťové logy zajistěte v rámci komunikace Microsoft Exchange Server z a do veřejné sítě Internet, a to za období nejméně 24 hodin před nelegitimním nahráním nebo upravením souboru až do vydání tohoto reaktivního opatření. Takto zajištěné informace neprodleně zašlete Úřadu,

    g) po dokončení všech předchozích úkonů proveďte bezpečnostní aktualizace Microsoft Exchange Server opravující zranitelnosti označené jako

CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 a CVE-2021-26858. Tento úkon proveďte nejpozději do 3 dnů od vydání tohoto reaktivního opatření,

h) po dokončení bezpečnostní aktualizace Microsoft Exchange Server opravující zranitelnosti označené jako CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 a CVE-2021-26858 bez ohledu na pozitivní nebo negativní nálezy v rámci předchozích úkonů zahajte bezpečnostní audit vnitřní sítě, jíž je Microsoft Exchange Server součástí. V rámci bezpečnostního auditu je nezbytné provést především audit doménových účtů zejména na přítomnost nelegitimních účtů, na podezřelý přístup ke stávajícím účtům (např. přihlášení v nestandardní dobu, přístupy k neobvyklým službám nebo adresářům, změny hesel), prověření nelegitimní komunikace Microsoft Exchange Server v rámci vnitřní sítě, zejména na doménový řadič, a na známky neautorizovaného přístupu nebo pokusy o něj na zařízeních v rámci vnitřní sítě. Bezpečnostní audit zahajte neprodleně po bezpečnostní aktualizaci Microsoft Exchange Server.

3) V případě, že v souladu s bodem 1) neidentifikujete Microsoft Exchange Server, zašlete tuto informaci neprodleně Úřadu.

Síťové indikátory kompromitace uvedené v bodě 2) písm. c):

- 103.77.192[.]219
- 104.140.114[.]110
- 104.250.191[.]110
- 108.61.246[.]56
- 149.28.14[.]163
- 157.230.221[.]198
- 167.99.168[.]251
- 185.250.151[.]72
- 192.81.208[.]169
- 203.160.69[.]66
- 211.56.98[.]146
- 5.254.43[.]18
- 80.92.205[.]81
- 165.232.154[.]116
- 104.248.49[.]97
- 5.2.69[.]13
- 91.192.103[.]43
- 161.35.45[.]41
- 45.77.252[.]175
- 1.36.203[.]86
- 1.65.152[.]106
- 103.212.223[.]210
- 104.225.219[.]16
- 108.172.93[.]199
- 110.36.235[.]230
- 110.36.238[.]2
- 110.39.189[.]202
- 112.168.90[.]84
- 114.205.37[.]150
- 116.49.101[.]143
- 117.146.53[.]162
- 119.197.26[.]38
- 119.231.129[.]222
- 121.154.50[.]51
- 121.174.31[.]220
- 121.176.145[.]25
- 122.213.178[.]102
- 123.16.231[.]247
- 124.5.24[.]161
- 139.59.56[.]239
- 161.35.76[.]1
- 167.179.67[.]3
- 170.10.228[.]74
- 172.105.87[.]139
- 179.1.65[.]54
- 182.165.53[.]4
- 185.171.166[.]188
- 185.224.83[.]137
- 200.52.177[.]138
- 201.17.196[.]211
- 201.208.18[.]226
- 202.182.118[.]99
- 209.58.163[.]131
- 211.177.182[.]80
- 213.219.235[.]158
- 218.39.251[.]104
- 219.100.37[.]239
- 219.100.37[.]243
- 219.78.205[.]63
- 23.95.80[.]191
- 31.182.197[.]163
- 31.28.31[.]132
- 34.87.189[.]145
- 39.123.17[.]120
- 46.101.232[.]43
- 46.23.196[.]21
- 49.36.47[.]211
- 58.126.135[.]235
- 58.190.46[.]175
- 61.82.150[.]49
- 78.188.104[.]84
- 78.189.225[.]136
- 86.105.18[.]116
- 89.147.119[.]227
- 90.230.190[.]92
- 1.9.2[.]18
- 103.135.248[.]70
- 108.61.171[.]184
- 113.173.3[.]225
- 128.90.21[.]223
- 159.89.95[.]163
- 182.18.152[.]105
- 185.65.134[.]165
- 185.65.134[.]170
- 34.87.113[.]30
- 46.244.29[.]17
- 5.189.162[.]164
- 5.2.69[.]14
- 130.255.189[.]21

Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, které některé výše uvedené úkony provedly v období od 3. března 2021 do vydání tohoto reaktivního opatření, nemusí tyto konkrétní úkony provádět opakovaně. Informaci o provedení jednotlivých úkonů a způsobu jejich provedení tyto orgány a osoby oznámí Úřadu.

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 po provedení všech uložených úkonů (tj. po zahájení bezpečnostního auditu podle bodu 2 písm. h) nebo po neidentifikování Microsoft Exchange Server v souladu s bodem 3).

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 k vydání tohoto opatření obecné povahy za 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 zjištění závažných zranitelností postihujících Microsoft Exchange Server, které byly označeny jako CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 a CVE-2021-26858. V návaznosti na tato zjištění vydal Úřad dne 3. března 2021 na svých internetových stránkách nejprve prvotní upozornění (https://www.nukib.cz/cs/infoservis/hrozby/1690-upozorneni-na-zranitelnosti-exchange-server/), které následně dne 4. března 2021 a 8. března 2021 dále aktualizoval. V rámci upozornění Úřad uvedl, že zjištěné zranitelnosti se týkají Microsoft Exchange Server 2010, 2013, 2016 a 2019 a zdůraznil nutnost jejich aktualizace.

2. I přes toto upozornění Úřad zjistil stále přetrvávající vysoké množství neaktualizovaných systémů, což významně zvyšuje riziko vážných útoků prostřednictvím využití této zranitelnosti Microsoft Exchange Server v České republice. S ohledem na povahu a význam výše uvedených zranitelností má Úřad důvodné podezření, že zranitelnost Microsoft Exchange Server může být plošně zneužita zejména k rozsáhlým ransomware útokům jak přímo ze strany kyberkriminálních skupin nebo jednotlivců, tak ve formě ransomware nebo access-as-a-service, kdy kyberkriminální skupiny za poplatek poskytují svůj získaný přístup do sítí obětí třetím stranám.

3. Je také nutno mít na paměti, že vláda České republiky vyhlásila z důvodu ohrožení zdraví v souvislosti s prokázáním výskytu koronaviru (označovaný jako SARS CoV-2) na území České republiky nouzový stav na dobu 30 dnů od 27. února 2021, 00:00 hodin. Důvodem pro vyhlášení nového nouzového stavu je velmi špatná epidemická situace způsobená především rychlým šířením tzv. britské mutace koronaviru SARS CoV-2 a potvrzeným výskytem velmi nebezpečné jihoafrické mutace viru, stejně tak jako kritická situace ve

zdravotnických zařízeních, které jsou přetíženy náporem těžkých případů pacientů s onemocněním covid-19. Tato situace klade zvýšené nároky na fungování důležitých organizací a institucí, především těch, které tvoří kritickou infrastrukturu státu. Z pohledu zákona o kybernetické bezpečnosti, který *„nedopadá na veškeré informační systémy, resp. služby a sítě elektronických komunikací, ale zaměřuje se pouze na ty informační a komunikační systémy, které mají aktuálně vzhledem ke shora uvedenému účelu zákona zásadní význam“* (cit. odůvodnění k návrhu zákona o kybernetické bezpečnosti), je pak nutné v takové situaci o to více klást důraz na zajištění fungování nejen kritické infrastruktury, ale všech orgánů a osob spadajících pod tento zákon.

4. 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.

5. 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 infrastruktury, významného informačního systému nebo informačního systému základní služby s výjimkou těch případů, kdy orgán nebo osoba v období od 3. března 2021 do vydání tohoto reaktivního opatření nahlásily Úřadu kybernetický bezpečnostní incident týkající se Microsoft Exchange Server. Reaktivní opatření tedy musí provést také takový orgán nebo osoba, který v souvislosti s Microsoft Exchange Server Úřadu incident hlásil, ale jen za předpokladu že disponuje ještě jiným Microsoft Exchange Server splňujícím definici v úvodu reaktivního opatření, u kterého incident doposud hlášen nebyl.

6. 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 současného nouzového stavu se tedy povinnost osob podle § 3 písm. a) a b) provést reaktivní opatření neuplatní.

7. 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 způsobeným realizací situace uvedené v bodu 2. tohoto odůvodnění. Úkony uložené ve výroku tohoto opatření obecné povahy vycházejí především z nutnosti identifikace, zda je v organizaci takový Microsoft Exchange Server, na který je možné uplatnit další úkony uložené v tomto reaktivním opatření. Jde především o skutečnost, že možnost uložení reaktivního opatření je realizovatelná jen vůči informačním nebo komunikačním systémům kritické informační infrastruktury, významným informačním systémům a informačním systémům základní služby. Z tohoto důvodu mohou být uloženy jen takové úkony, které směřují k zabezpečení těchto systémů před kybernetickým bezpečnostním incidentem. Z tohoto důvodu je proto nutné vymezit, o které Microsoft Exchange Server se jedná. Za tím účelem obsahuje bod 1) výroku definici relevantních Microsoft Exchange Server.

8. V případě, že orgán nebo osoba identifikuje relevantní Microsoft Exchange Server, jsou mu reaktivním opatřením uloženy další podrobné úkony směřující k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem.

9. Součástí uložených úkonů je zaslání rozsahu veřejných DNS záznamů nebo veřejných IP adres zjištěných Microsoft Exchange Server podle bodu 1) výroku tohoto reaktivního opatření. Tyto informace jsou již nyní dobrovolnou součástí hlášení kontaktních údajů, které orgány a osoby podle zákona o kybernetické bezpečnosti zasílají Úřadu. V rámci tohoto reaktivního opatření směřujícího k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem je tento úkon uložen pro zjištěné Microsoft Exchange Server 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 řešených zranitelností a hodnocení s nimi souvisejících hrozeb. Tyto výstupy je potřeba neprodleně zaslat na cert.incident@nukib.cz.

10. Dalším z uložených úkonů je použití nástroje „Test-ProxyLogon.ps1“, který slouží k identifikaci zneužití zranitelností označených jako CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 a CVE-2021-26858. Použití tohoto konkrétního nástroje je uloženo, protože jde o nástroj dodávaný přímo výrobcem systému (Microsoft) v návaznosti na zjištění výše uvedených zranitelností. Podrobnější informace o detailním použití tohoto nástroje naleznete na internetových stránkách:

    https://github.com/microsoft/CSS-Exchange/tree/main/Security#test-proxylogonps1.

    V případě pozitivního nálezu je nezbytné zajistit výstup z nástroje „Test-ProxyLogon.ps1“ a tyto výstupy neprodleně zaslat na cert.incident@nukib.cz.

11. Dalším uloženým úkonem je prověření uvedených síťových indikátorů kompromitace. Jedná se o soubor indikátorů dostupných jednak z veřejných zdrojů, jednak z vlastní činnosti Úřadu. Tyto výstupy je potřeba neprodleně zaslat na cert.incident@nukib.cz.

12. Dalším uloženým úkonem je vyhledání nelegitimně nahraných nebo upravených souborů (zejména ASPX, PHP, JS) v souborovém systému Microsoft Exchange Server. Předmětem vyhledání jsou soubory nahrané útočníkem, které nejsou součástí originální instalace Microsoft Exchange Server.

    Vyhledání lze provést buďto pomocí veřejně dostupných nástrojů (více informací je dostupných např. na https://github.com/cert-lv/exchange_webshell_detection nebo https://github.com/microsoft/CSS-Exchange/blob/main/Security/Defender-MSERT-Guidance.md), nebo je potřeba uvedené soubory vyhledat manuálně.

    Podle aktuálně dostupných informací se tyto závadné soubory nejčastěji vyskytují v následujících adresářích:

    - %IIS installation path%\aspnet_client*
    - %IIS installation path%\aspnet_client\system_web*
    - %Exchange Server installation path%\FrontEnd\HttpProxy\owa\auth*
    - %Exchange Server Installation%\FrontEnd\HttpProxy\ecp\auth*

    Takto získané informace Úřad potřebuje k identifikaci podoby konkrétních způsobů zneužití uvedených zranitelností a k plnění dalších zákonných povinností Úřadu (zejm. preventivní a metodické činnosti, analýzy a monitoringu kybernetických hrozeb a rizik atd.). Tyto výstupy je potřeba neprodleně zaslat na cert.incident@nukib.cz.

13. Nalezení nelegitimně nahraného nebo upraveného souboru v rámci úkonu podle bodu 2) písm. d) výroku je známkou kompromitace systému. Z tohoto důvodu je potřeba zajistit informace k analýze aktivity útočníka na Microsoft Exchange Server, a to pomocí ECP logů, HTTP logů, Windows Event logů a exportu registrových klíčů, protože tyto jsou schopny poskytnout bližší informace v souvislosti se zneužitím předmětných zranitelností. Tyto výstupy je potřeba neprodleně zaslat na cert.incident@nukib.cz. Zajištění logů lze nahradit zajištěním forenzního obrazu disku a paměti serveru. Tento postup je Úřadem preferován. V případě, že shromážděné informace není možné z důvodu jejich rozsahu či formátu (např. v případě objemu většího než 10 MB dat) zaslat na uvedenou e-mailovou adresu, je potřeba kontaktovat Úřad (na stejné e-mailové adrese) a dohodnout náhradní způsob předání.

14. K bližší analýze aktivity útočníka na Microsoft Exchange Server je dále potřeba zajištění logů síťového provozu Microsoft Exchange Server z a do veřejné sítě Internet, které umožní identifikovat zdroj kompromitace a následnou činnost. Časový rozsah stanovený ve výroku reaktivního opatření směřuje k tomu zjistit, zda útočník nevyvíjel aktivitu již

před samotnou kompromitací, stejně tak jako slouží k tomu, aby bylo možné analyzovat všechny jeho následné činnosti. Tyto výstupy je potřeba neprodleně zaslat na cert.incident@nukib.cz. V případě, že shromážděné informace není možné z důvodu jejich rozsahu či formátu (např. v případě objemu většího než 10 MB dat) zaslat na uvedenou e-mailovou adresu, je potřeba kontaktovat Úřad (na stejné e-mailové adrese) a dohodnout náhradní způsob předání.

15. Další podpůrné informace k realizaci některých výše uvedených úkonů naleznete také zde:

    https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

16. Jako další uloženou povinnost je potřeba provést bezpečnostní aktualizace Microsoft Exchange Server opravující zranitelnosti označené jako CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 a CVE-2021-26858**. Tento úkon je nezbytné provést až po provedení všech předchozích úkonů, neboť v případě, že bude proveden dřív, může dojít ke ztrátě informací o kompromitaci, potřebných pro splnění předchozích úkonů.** Nanejvýš lze provést tento úkon paralelně, např. vytvořením kopie Microsoft Exchange Server, ze které lze následně zajistit potřebná data o kompromitaci bez rizika jejich ztráty při aktualizaci. Tento úkon je však potřeba provést neprodleně, nejpozději do tří dnů v případě, kdy k odkladu provedení úkonu existují objektivní důvody.

17. Protože zranitelnost umožňuje útočníkům získat na Microsoft Exchange Server systémová oprávnění, je potřeba provést bezpečnostní audit se zaměřením na nejčastější vektory útoku v rámci interní sítě.

18. 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. Podle § 13 odst. 4 zákona o kybernetické bezpečnosti stanoví náležitosti oznámení prováděcí právní předpis.

19. Podle § 33 odst. 2 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), 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/

20. Provedení reaktivního opatření oznámí dotčené orgány a osoby Úřadu i v případě, že věcně nebudou jednotlivé úkony reaktivního opatření pro jejich informační systémy a služby a sítě elektronických komunikací relevantní (např. nebudou plnit úkony v bodu 2)

výroku reaktivního opatření, protože nebude využívat Microsoft Exchange Server 2010, 2013, 2016, ani 2019). V takovém případě tyto orgány a osoby oznámí Úřadu tuto skutečnost v souladu s bodem 3) výroku reaktivního opatření.

21. 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, 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.

22. 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.

23. 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 tiskového mluvčího 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: 11.03.2021 21:19

NÚKIB

Ing. Karel Řehka
ředitel
elektronicky podepsáno

Vyvěšeno dne: .....

Sejmuto dne: .....