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

Spisová značka:
350 - 949/2020
Číslo jednací:
6563/2020-NÚKIB-E/350

Brno, 16. prosince 2020

Vyřizuje:
Vladěna Sasková

VEŘEJNÁ VYHLÁŠKA

OPATŘENÍ OBECNÉ POVAHY

Národní úřad pro kybernetickou a informační bezpečnost se sídlem Brno, Mučednická 1125/31, PSČ 616 00 (dále též 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 o kybernetické bezpečnosti a § 171, § 173 a § 174 zákona č. 500/2004 Sb., správního řádu, ve znění pozdějších předpisů, toto **reaktivní opatření k řešení kybernetického bezpečnostního incidentu a současně 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 provést ve stanovené lhůtě:**

1. **Provést aktualizaci využívaných aplikací platformy Orion společnosti SolarWinds podle pokynů uveřejněných na internetových stránkách této společnosti (dostupné zde: https://www.solarwinds.com/securityadvisory), a to minimálně v rozsahu následujících aplikací:**

    a. Network Performance Monitor
    b. Server and Application Monitor
    c. Network Configuration Manager
    d. Virtualization Manager
    e. NetFlow Traffic Analyzer
    f. Log Analyzer
    g. Storage Resource Monitor
    h. IP Address Manager

i. VoIP and Network Quality Manager
j. User Device Tracker
k. Server Configuration Monitor
l. Web Performance Monitor
m. Database Performance Analyzer
n. Patch Manager

Tento úkon jsou povinné osoby povinny provést bezodkladně po nabytí účinnosti tohoto opatření obecné povahy, nejpozději však do 6 dnů ode dne nabytí účinnosti tohoto opatření obecné povahy.

2. **U informačních systémů a sítí elektronických komunikací, které mají implementovány či využívají aplikace platformy Orion společnosti SolarWinds, prověřit indikátory kompromitace, které jsou uvedeny v tomto opatření obecné povahy, a další indikátory kompromitace, které budou Úřadem bezodkladně po jejich zjištění uveřejněny na internetových stránkách www.nukib.cz (konkrétně zde: https://www.nukib.cz/cs/infoservis/hrozby/), a neprodleně informovat Úřad o pozitivních nálezech**.

   Indikátory kompromitace, které je povinná osoba povinna prověřit bezodkladně po nabytí účinnosti tohoto opatření obecné povahy, nejpozději však do 1 týdne ode dne nabytí účinnosti tohoto opatření obecné povahy:

SHA256	Verze souboru	První výskyt
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	2019.4.5200.9083	Březen 2020
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	2020.2.100.12219	Březen 2020
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	2020.2.100.11831	Březen 2020
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	N/A	Březen 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	Duben 2020
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2020.2.5200.12394	Duben 2020
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	2020.2.5300.12432	Květen 2020
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	2019.4.5200.8890	Říjen 2019
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	2019.4.5200.8890	Říjen 2019

d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600	N/A	N/A
53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7	N/A	N/A
292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712	N/A	N/A
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	N/A	N/A

Síťové indikátory kompromitace – nutno prověřit komunikaci na IP a domény:

13.57.184[.]217
13.59.205[.]66
18.217.225[.]111
18.220.219[.]143
196.203.11[.]89
3.16.81[.]254
3.87.182[.]149
3.87.182[.]149
34.219.234[.]134
54.193.127[.]66
54.215.192[.]52
34.203.203[.]23
139.99.115[.]204
5.252.177[.]25
5.252.177[.]21
204.188.205[.]176
51.89.125[.]18
167.114.213[.]199

avsvmcloud[.]com
deftsecurity[.]com
digitalcollege[.]org
freescanonline[.]com
globalnetworkissues[.]com
kubecloud[.]com
lcomputers[.]com
seobundlekit[.]com
solartrackingsystem[.]net
thedoccloud[.]com
virtualwebdata[.]com
webcodez[.]com
websitetheme[.]com

highdatabase[.]com
incomeupdate[.]com
databasegalore[.]com
panhardware[.]com
zuzpertech[.]com

Další indikátory kompromitace, které budou Úřadem bezodkladně po jejich zjištění uveřejněny na internetových stránkách www.nukib.cz (konkrétně zde: https://www.nukib.cz/cs/infoservis/hrozby/), je povinná osoba povinna prověřit bezodkladně po seznámení se s nimi, nejpozději však do 1 týdne od jejich uveřejnění.

Jelikož některé indikátory kompromitace mohou náležet známým VPN providerům, povinná osoba u případných pozitivních nálezů prověří, zda se opravdu jedná o podezřelou komunikaci (např. navázání relace, odesílání dat, komunikace z vnitřní sítě), a pouze takto posouzené pozitivní záchyty oznámí Úřadu. O podezřelou komunikaci se nejedná např. u skenování perimetru apod.

Prověření výše popsaných **síťových** indikátorů kompromitace je vzhledem k době trvání kompromitace nezbytné provést ve vztahu k provozu od března 2020 včetně.

3. **V případě, že povinná osoba využívá či má ve svých informačních systémech a sítích elektronických komunikací implementovány aplikace platformy Orion společnosti SolarWinds, provést prověření bezpečnosti informačních systémů a sítí elektronických komunikací, a to minimálně v níže uvedeném rozsahu, a v návaznosti na výsledky prověření bezpečnosti zavést přiměřená bezpečnostní opatření ke zvýšení zabezpečení informačního systému nebo sítí elektronických komunikací a k zamezení realizace či dalšího pokračování zjištěné kompromitace systému nebo sítí.**

   Minimální rozsah prověření bezpečnosti a přijetí bezpečnostních opatření je stanoven následovně:

   a. Prověření indikátorů kompromitace podle bodu 2 výroku.

   b. Na v bodu 1 jmenovaných produktech společnosti SolarWinds reset hesel u všech účtů.

   c. Přistupovat k informačním systémům a sítím elektronických komunikací, které mají v infrastruktuře vazbu na software uvedený v bodě 1 výroku, jako k potenciálně kompromitovaným a dbát tedy na zvýšený monitoring podezřelého chování.

   d. Přistupovat ke každému účtu na platformě Orion jako k potenciálně kompromitovanému a provést audit všech přihlašovacích údajů a jejich změnu napříč institucí.

   e. Provedení revize účtů na systémech a sítích uvedených v písmenu c) tohoto bodu výroku.

f. Na systémech a sítích uvedených v písmenu c) tohoto bodu výroku prověření nejčastějších persistenčních mechanismů (viz https://attack.mitre.org/tactics/TA0003/).

g. Ověření anomálií v provozu od března 2020 do současnosti (exfiltrace dat v nezvyklé hodiny a na neobvyklé adresy) na všech sítí a nejen na těch, na kterých je provozován software platformy Orion společnosti SolarWinds.

Tento úkon jsou povinné osoby povinny provést bezodkladně po nabytí účinnosti tohoto opatření obecné povahy, nejpozději však zahájí provádění celého rozsahu úkonu do 1 týdne ode dne nabytí účinnosti tohoto opatření obecné povahy.

Nad rámec výše uvedeného doporučujeme zvážení izolace všech aktivních služeb Orion od veřejné sítě internet, a to až do doby provedení všech úkonů bodu 3 výroku a do zjištění, že je zajištěna bezpečnost informací v informačních systémech a sítích elektronických komunikací.

Tímto reaktivním opatřením jsou vázány orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti.

Toto reaktivní opatření je potřeba provést ve lhůtách k tomu určených u jednotlivých úkonů.

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, nejpozději však do 6 dnů od jeho provedení. V případě úkonu uvedeného v bodu 3 výroku oznámí povinná osoba bezodkladně, nejpozději do 6 dnů od učinění rozhodné skutečnosti, zahájení této činnosti, stejně jako její následné dokončení.

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 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“), dospěl k vydání tohoto opatření obecné povahy za účelem **řešení kybernetického bezpečnostního incidentu a současně 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 významných bezpečnostních rizik spojených se softwarem společnosti SolarWinds, konkrétně pak aplikacemi z jejich platformy Orion. Aktualizace aplikací uvedených v bodu 1 výroku tohoto opatření obecné povahy byly od března 2020 do současnosti kompromitovány a zákazníci využívající software platformy Orion společnosti SolarWinds byli a s vysokou pravděpodobností stále jsou vystaveni vysokému riziku kompromitace jejich sítí backdoorem SUNBURST. Útočníci jsou schopni po úspěšnému průniku do sítě oběti kompromitovat například široce používanou službu Office 365, čímž se mohou dostat do e-mailové komunikace oběti a k souborům uloženým v cloudovém úložišti.

Neaktualizovaný software z platformy Orion lze považovat za kompromitovaný, stejně jako celou síť, ve které je nasazený.

2. 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.

3. 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.

4. 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.

5. Reaktivní opatření, jak je specifikováno ve výroku tohoto opatření obecné povahy, obsahuje sadu úkonů, jejichž provedení je nezbytné k zamezení pokračování kybernetického bezpečnostního incidentu v potenciálně kompromitovaném informačním systému nebo síti elektronických komunikací a pro zajištění vyšší úrovně zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem způsobeným realizací rizika uvedeného v bodu 1 odůvodnění. Úkon uvedený v bodě 1 výroku je v současné době jediným známým efektivním nástrojem pro zamezení dalšího možného pokračování kybernetického bezpečnostního incidentu a pro zabezpečení informačních systémů a sítí elektronických komunikací před (dalším) výskytem incidentu (pomineme-li možnost úplného zamezení používání aplikací platformy Orion).

6. V případě úkonů uvedených v bodech 1 a 2 výroku tohoto opatření obecné povahy se jedná o úkony doporučené samotným výrobcem kompromitované platformy.

7. Úkonem pod bodem 3 výroku tohoto opatření obecné povahy Úřad zavazuje povinné osoby k provedení prověření bezpečnosti informačních systémů a sítí elektronických komunikací nad rámec úkonů uvedených v bodech 1 a 2 výroku. S ohledem na rozmanitost informačních

systémů a sítí elektronických komunikací povinných osob a nemožnost definice kompletního univerzálního způsobu provedení tohoto prověření bezpečnosti Úřad uvádí toliko minimální požadavky na podobu prověření bezpečnosti a přijetí bezpečnostních opatření. Jedná se o úkony, které korespondují se zákonnými povinnostmi povinných osob co do zavádění a provádění bezpečnostních opatření podle § 5 zákona o kybernetické bezpečnosti, a jejichž realizace by z toho důvodu neměla činit významnější problémy. Provedení dalších úkonů a zavedení dalších bezpečnostních opatření vyplyne z interních procesů povinné osoby a jejích pravidel pro řízení bezpečnosti informací.

8. Úřad dále důrazně doporučuje řídit se při provádění prověření bezpečnosti všemi doporučeními společnosti SolarWinds (dostupné zde: https://www.solarwinds.com/securityadvisory) a dále relevantními instrukcemi bezpečnostní společnosti FireEye, jež byla kybernetickým bezpečnostním incidentem popsaným v bodě 1 odůvodnění přímo dotčena (dostupné zde: https://github.com/fireeye/sunburst_countermeasures a zde: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html). Současně Úřad doporučuje při volbě konkrétního postupu zvážit též doporučení americké vládní agentury pro kybernetickou bezpečnost Cybersecurity and Infrastructure Security Agency (dostupné zde: https://cyber.dhs.gov/ed/21-01/).

9. 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.

10. 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/.

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

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: 16.12.2020 15:32

NÚKIB

Ing. Karel Řehka
ředitel
elektronicky podepsáno

Vyvěšeno dne: .....

Sejmuto dne: .....