ČNB ČESKÁ NÁRODNÍ BANKA
NA PŘÍKOPĚ 28
115 03 PRAHA 1

Sekce licenčních a sankčních řízení

V Praze dne 19. ledna 2023
Č.j.: 2023 / 9655 / 570
Sp.zn. Sp/2022/100/573
Počet stran: 25

P Ř Í K A Z

Česká národní banka (dále též „správní orgán“) jako orgán dohledu nad finančním trhem podle zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů (dále jen „zákon o ČNB“) a jako orgán dohledu nad bankami podle zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (dále jen „zákon o bankách“ nebo „ZoB“), dále provedený vyhláškou č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, ve znění pozdějších předpisů (dále jen „vyhláška č. 163/2014 Sb.“), rozhodla dle ustanovení § 90 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů (dále jen „přestupkový zákon“) ve spojení s ustanovením § 150 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“) v řízení vedeném se společností Raiffeisen stavební spořitelna a.s., IČO: 492 41 257, se sídlem Hvězdova 1716/2b, 140 78 Praha 4 - Nusle, takto:

Společnost Raiffeisen stavební spořitelna a.s., IČO: 492 41 257, se sídlem Hvězdova 1716/2b, 140 78 Praha 4 - Nusle se uznává vinnou, že v období od 1.1.2019 do 15.10.2021 nedisponovala řídicím a kontrolním systémem, který by byl účinný, ucelený a přiměřený charakteru, rozsahu a složitosti rizik spojených s modelem jejího podnikání a činností, a to v oblasti řízení rizik informačních systémů a informačních technologií, konkrétně v oblasti:

i) analýzy rizik,
ii) bezpečnostního monitoringu,
iii) ochrany proti pokročilým kybernetickým hrozbám,
iv) provozu informačních systémů
v) elektronického bankovnictví
vi) pohotovostních plánů,
vii) rekonstruovatelnosti auditorských spisů,

t e d y p o r u š i l a

povinnost dle ustanovení § 8b odst. 2 zákona o bankách,

č í m ž s e d o p u s t i l a

přestupku dle ustanovení § 36e odst. 2 písm. a) zákona o bankách,

z a c o ž s e j í u k l á d á

podle ustanovení § 36e odst. 6 písm. f) zákona o bankách pokuta ve výši 100 000 Kč (slovy jedno sto tisíc korun českých). Pokuta je splatná do 30 dnů od nabytí právní moci

tohoto příkazu na účet Celního úřadu pro hlavní město Prahu vedený u České národní banky, č. 3754-67724011/0710, konstantní symbol 1148, variabilní symbol je identifikační číslo plátce.

O D Ů V O D N Ě N Í

A. Identifikace účastníka řízení

1. Společnost Raiffeisen stavební spořitelna a.s., IČO: 492 41 257, se sídlem Hvězdova 1716/2b, 140 78 Praha 4 - Nusle (dále jen „účastník řízení“) je obchodní společností, která je ode dne 4.9.1993 zapsána v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. B 2102. Jediným akcionářem účastníka řízení je obchodní společnost Raiffeisenbank a.s., IČO: 492 40 901, se sídlem Hvězdova 1716/2b, 140 78 Praha 4 - Nusle (dále jen „RBCZ“).

2. Účastník řízení je dále zapsán v registru České národní banky ode dne 4.9.1993 jako banka provozující činnost stavební spořitelny podle zákona č. 96/1993 Sb., o stavebním spoření a státní podpoře stavebního spoření, ve znění pozdějších předpisů.[1]

B. Postup správního orgánu před vydáním příkazu

3. Dne 6.9.2021 zahájil správní orgán u účastníka řízení kontrolu, a to doručením oznámení o zahájení kontroly ze dne 3.9.2021, č. j. 2021/091687/CNB/580 (dále jen „Kontrola“).[2] Správní orgán v rámci Kontroly u účastníka řízení prověřoval dodržování právních předpisů v oblasti řízení rizik informačních systémů/informačních technologií (dále jen „IS/IT“) včetně outsourcingu, a to ode dne 1.1.2019.

4. V průběhu kontrolního období došlo k outsourcingu kontrolovaných činností do RBCZ, a to konkrétně k outsourcingu činností v oblasti informační bezpečnosti a kontinuity obchodní činnosti (z angl. *business continuity management*, dále jen „BCM“) s účinností od 1.6.2021[3] a k outsourcingu činnosti Odboru informačních technologií (dále jen „OIT“) a Analýzy a aplikačního vývoje (dále jen „OAV“) účastníka řízení s účinností od 1.9.2021.[4] S ohledem na termín zahájení poskytování činností v oblasti informační bezpečnosti a BCM, OIT a OAV v RBCZ a na termín zahájení Kontroly nebylo možné zjistit stav plnění požadavků stanovených na řídicí a kontrolní systém a jeho součásti, plnění předpokladů řádné správy a řízení prostřednictvím uplatňovaných řádných postupů v této oblasti Kontroly po zahájení poskytování výše uvedených činností v RBCZ. Z těchto důvodů se proto správní orgán v rámci Kontroly zaměřil především na období od 1.1.2019 do předání a zahájení uvedených činností v RBCZ.

---

[1] Dostupné z evidence České národní banky zde: https://apl.cnb.cz/apljerrsdad/JERRS.WEB10.VIZITKA?p_lang=cz&p_SEQ_ID=125&p_VER_ID=1011&p_DATUM=26.04.2022&p_ROL_KOD=.

[2] Oznámení o zahájení kontroly ze dne 3.9.2021, č. j. 2021/091687/CNB/580, s doručenkou. Viz soubor „*2021_091687_CNB_580_RSTS_Oznameni_o_zahajeni_kontroly_vyzva_a_pouceni.pdf*“, spis, č. l. 5 (DVD).

[3] Smlouva o poskytování služeb uzavřená mezi RBCZ a účastníkem řízení dne 31. 5. 2021. Viz soubory „*Smlouva o poskytování služeb CDR17927.pdf*“ a „*Smlouva o poskytování služeb CDR17927 Zvláštní smlouva.pdf*“, vše spis, č. l. 5 (DVD).

[4] Smlouva o poskytování služeb Analýzy a aplikačního vývoje “OAV“ ze dne 31.8.2021, viz soubor „*3031 OAV.pdf*“ a Smlouva o poskytování služeb „Odboru informačních technologií“ (OIT) ze dne 31.8.2021, viz soubor „*3032 OIT.pdf*“, vše spis, č. l. 5 (DVD).

5. Na základě Kontroly byly zjištěny nedostatky spočívající v porušení povinností uložených účastníku řízení zákonem o bankách, resp. vyhláškou č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstvech a obchodníků s cennými papíry, ve znění pozdějších předpisů (dále jen „vyhláška č. 163/2014 Sb.), které byly uvedeny v protokolu o kontrole ze dne 7.2.2022, č. j. 2022/013700/CNB/580 (dále jen „Protokol“).[5]

C. Skutková zjištění a právní posouzení správního orgánu

6. Podle ustanovení § 8b odst. 1 písm. b) ZoB musí mít banka řídicí a kontrolní systém, který zahrnuje systém řízení rizik, který vždy zahrnuje 1. pravidla přístupu banky k rizikům, kterým banka je nebo může být vystavena, včetně rizik vyplývajících z vnějšího prostředí a rizika likvidity, 2. účinné postupy rozpoznávání, vyhodnocování, měření, sledování a ohlašování rizik, a 3. účinné postupy přijímání opatření vedoucích k omezení případných rizik.

7. Podle ustanovení § 8b odst. 1 písm. c) ZoB musí mít banka řídicí a kontrolní systém, který zahrnuje systém vnitřní kontroly, jehož součástí je vždy 1. vnitřní audit a 2. průběžná kontrola dodržování právních povinností a povinností plynoucích z vnitřních předpisů banky.

8. Podle ustanovení § 8b odst. 2 ZoB musí být řídicí a kontrolní systém účinný, ucelený a přiměřený povaze, rozsahu a složitosti rizik spojených s modelem podnikání a činností banky v jeho celku i částech.

9. Podle ustanovení § 8b odst. 9 ZoB Česká národní banka stanoví vyhláškou podrobnější požadavky na řídicí a kontrolní systém na individuálním i konsolidovaném nebo subkonsolidovaném základě v mezích podle odstavce 1, včetně působností, pravomocí, složení a fungování orgánů a výborů, jakož i požadavků na jejich členy, pokud toto není upraveno přímo použitelným předpisem Evropské unie upravujícím obezřetnostní požadavky, nařízením nebo rozhodnutím Evropské komise.

10. Podrobnější požadavky na systém řízení rizik bank jsou v souladu s výše uvedeným stanoveny ve vyhlášce č. 163/2014 Sb. Vyhláška č. 163/2014 Sb. se použije pro účastníka řízení jako povinnou osobu ve smyslu ustanovení § 2 této vyhlášky.

i) <u>Analýza rizik spjatých s IS/IT</u>

11. Správní orgán vyzval účastníka řízení k předložení všech vnitřních předpisů a dokumentů, které se vztahují ke kontrolovaným oblastem činnosti účastníka řízení.[6] Účastník řízení v rámci své odpovědi na výzvu správního orgánu předložil zejména následující dokumenty, které se vztahují k analýze rizik IS/IT informačních aktiv a návazné plány na zvládání identifikovaných rizik:

[5] Protokol o kontrole ze dne 8.2.2022, č. j. 2022/013700/CNB/580. Viz soubor „*2022_013700_CNB_580_RSTS_Protokol_Rizeni_rizik_ISIT.pdf*“, spis, č. l. 5 (DVD).

[6] Oznámení o zahájení kontroly a výzva k poskytnutí podkladů a informací ze dne 3.9.2021, č. j. 2021/091687/CNB/580, bod A.12.
Viz soubor „*2021_091687_CNB_580_RSTS_Oznameni_o_zahajeni_kontroly_vyzva_a_pouceni.pdf*“, spis, č. l. 5 (DVD).

- *Bezpečnostní politika IS/IT* účastníka řízení v. 3[7], v. 4[8] a v. 5[9]
- *Klasifikace informačních aktiv* v. 3[10] a v. 4[11]
- Soubor „*IT_risk_points_2021.xlsx*“[12]

12. Při stanovení požadavků na řídicí a kontrolní systém v jednotlivých oblastech řízení bezpečnosti přihlížel účastník řízení mj. taktéž k požadavkům stanoveným ve standardech skupiny Raiffeisen Bank International (dále jen „RBI“). Správní orgán konstatuje, že předmětem Kontroly nebylo vyhodnocení plnění skupinových standardů RBI a že v rámci Kontroly vycházel z vnitřních předpisů předložených účastníkem řízení.

a) Vnitřní předpisy pro oblast analýzy bezpečnostních rizik spjatých s provozem IS/IT účastníka řízení

13. Podle ustanovení § 10 odst. 1 vyhlášky č. 163/2014 Sb. povinná osoba zajistí, že požadavky stanovené na řídicí a kontrolní systém a jeho součásti a postupy povinné osoby k jejich splnění a při výkonu dalších činností jsou promítnuty do vnitřních předpisů povinné osoby. Povinná osoba stanoví postup při přijímání, změně a uplatňování vnitřních předpisů.

14. Ze znění ustanovení kap. 4 písm. b) *Bezpečnostní politiky IS/IT* účastníka řízení v.3, v. 4 i v. 5 mj. vyplývá, že nedílnou součástí organizace a řízení bezpečnosti IS/IT účastníka řízení je komplexní analýza bezpečnostních rizik spjatých s provozem IS/IT. Účastník řízení dále v této kapitole stanovil následující požadavky na komplexní analýzu bezpečnostních rizik spjatých s provozem:

c) V rámci zmíněné komplexní analýzy rizik IS/ICT RSTS banka vždy identifikuje a definuje:

i. veškerá primární i sekundární aktiva IS/ICT RSTS, vazby mezi nimi,

ii. hrozby, které působí na aktiva IS/ICT RSTS,

iii. slabá zranitelná místa,

iv. pravděpodobnost realizace hrozby a odhad jejich následků.

d) Analýza rizik a odhad následků při implementaci nového systému (subsystému, aplikace atd.) nebo změně stávající architektury IS/ICT RSTS jsou provedeny ještě před samotnou realizací této implementace nebo změny. Děje se tak vždy v souladu se závaznými pravidly změnového a projektového řízení definovanými příslušnými vnitřními předpisy. K identifikaci rizik, zranitelných míst, pravděpodobnosti defaultu a odhadu následků rizika slouží postupy a metody stanovené příslušnými vnitřními předpisy.

---

[7] Příkaz č. 01/2012 *Bezpečnostní politika informačních systémů a informačních technologií*, verze č. 4, účinná od blíže nespecifikovaného data roku 2017. Viz soubor „*P 2012-01 Bezpečnostní politika IS IT RSTS - verze 3_final.doc*“, spis, č. l. 5 (DVD).

[8] Příkaz č. 01/2012 *Bezpečnostní politika informačních systémů a informačních technologií*, verze č. 4, účinná od 3.9.2019. Viz soubor „*P 2012-01 Bezpečnostní politika IS, IT RSTS V4.docx*“, spis, č. l. 5 (DVD).

[9] Příkaz č. 01/2012 *Bezpečnostní politika informačních systémů a informačních technologií*, verze č. 5, účinná od 21.9.2021. Viz soubor „*P 2012-01 Bezpečnostní politka IS, IT RSTS V5.docx*“, spis, č. l. 5 (DVD).

[10] Příkaz č. 06/2018 *Klasifikace informačních aktiv*, verze č. 3, účinná od 28.4.2020. Viz soubor „*P 2018-06 Klasifikace informačních aktiv V3.docx*“, spis, č. l. 5 (DVD).

[11] Příkaz č. 06/2018 *Klasifikace informačních aktiv*, verze č. 4, účinná od 21.9.2021. Viz soubor „*P 2018-06 Klasifikace informačních aktiv V4.docx*“, spis, č. l. 5 (DVD).

[12] Spis, č. l. 5 (DVD).

15. Správní orgán v průběhu Kontroly na místě opakovaně vyzval[13] účastníka řízení k upřesnění, kterými vnitřními předpisy stanovil postupy a metody k identifikaci rizik, zranitelných míst, pravděpodobnosti defaultu a odhadu následků rizika tak, jak vyplývá z výše uvedeného ustanovení *Bezpečnostní politiky IS/IT* účastníka řízení.

16. V průběhu Kontroly správní orgán zjistil, že s výjimkou vnitřních předpisů uvedených výše v odst. 11 tohoto příkazu nebyla oblast komplexní analýzy bezpečnostních rizik spjatých s provozem IS/IT účastníka řízení upravena dalšími vnitřními předpisy. **Účastník řízení tak neměl jednoznačně stanoveno, která z rolí definovaných ve vnitřních předpisech je odpovědná za provedení analýzy rizik, rozsahu a frekvence provedení této analýzy, požadavky na dokumentaci a navazující činnosti.**

17. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[14] do 31.5.2021[15] nevypracoval pravidla a postupy pro komplexní analýzu bezpečnostních rizik spjatých s IS/IT, když nestanovil, která z rolí je odpovědná za provedení analýzy rizik, rozsah a frekvenci provedení této analýzy a požadavky na dokumentaci, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 10 odst. 1 vyhlášky č. 163/2014 Sb.**

b) Požadavky na procesy posouzení rizik, přezkumy, hodnocení a testování bezpečnosti informací

18. Podle ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. povinná osoba zabezpečí, že proces rozpoznávání rizik je zajištěn u všech činností a na všech řídicích a organizačních úrovních a umožňuje odhalování nových, dosud neidentifikovaných rizik.

19. Správní orgán přezkoumal obsah předložených vnitřních předpisů uvedených výše v odst. 11 tohoto příkazu a dospěl k závěru, že účastník řízení v nich nezapracoval požadavky vyplývající z kap. 1.4.6 Obecných pokynů Evropského orgánu pro bankovnictví pro řízení rizik v oblasti IKT a bezpečnosti ze dne 28.11.2019 (dále jen „Obecné pokyny EBA/GL/2019/04“),[16] které jsou pro účastníka řízení závazné ve smyslu čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24.11.2010, o zřízení Evropského orgánu dohledu. Jedná se o požadavky na procesy posouzení rizik, přezkumy, hodnocení a testování bezpečnosti informací. Tyto oblasti nebyly v předložených vnitřních předpisech zapracovány.

20. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 30.6.2020[17] do 31.5.2021[18] nezapracoval do svých vnitřních předpisů požadavky na procesy posouzení rizik, přezkumy, hodnocení a testování bezpečnosti informací vyplývající, čímž postupoval v rozporu s požadavkem upřesněným**

---

[13] E-mail správního orgánu účastníkovi řízení ze dne 4.11.2021. Viz soubor „*Email_CNB_20211104*“, spis, č. l. 5 (DVD).
[14] Počátek kontrolního období.
[15] Poslední den před provedením outsourcingu do RBCZ.
[16] Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880808/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_CS.pdf.
[17] Datum účinnosti Obecných pokynů EBA/GL/2019/04.
[18] Poslední den před provedením outsourcingu do RBCZ.

v ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. ve spojení s kapitolou 1.4.6. Obecných pokynů EBA/GL/2019/04.

c) Provádění komplexní analýzy bezpečnostních rizik spjatých s provozem IS/IT

21. Podle ustanovení bodu 17 přílohy č. 6 k vyhlášce č. 163/2014 Sb. povinná osoba provede analýzu rizik spjatých s informačními systémy. V ní definuje aktiva informačních systémů, hrozby, které na ně působí, zranitelná místa informačních systémů, pravděpodobnost realizace hrozeb a odhad jejich následků a protiopatření. Povinná osoba pravidelně provádí aktualizaci analýzy rizik spjatých s informačními systémy.

22. Vzhledem ke skutečnosti, že předložený soubor „*IT_risk_points_2021.xlsx*" neodpovídal dle vyhodnocení správního orgánu výše uvedeným požadavkům stanoveným v *Bezpečnostní politice IS/IT* účastníka řízení, stejně jako neodpovídal požadavku na provedení analýzy rizik spjatých s informačními systémy dle ustanovení bodu 17 přílohy č. 6 k vyhlášce č. 163/2014 Sb., vyzval správní orgán účastníka řízení ke sdělení, zda byla provedena komplexní analýza bezpečnostních rizik spjatých s provozem IS/IT účastníka řízení a aby předložil její výsledek za období 2019 – 2021.[19]

23. Dne 8.11.2021 zaslal účastník řízení správnímu orgánu následující vyjádření týkající se požadavku na předložení výsledků komplexní analýzy bezpečnostních rizik spjatých s provozem IS/IT účastníka řízení za období 2019 – 2021: *„Nejblíže tomu má analýza rizik, kterou provádělo OŘR* [Odbor řízení rizik]. *Příklad zasílám v příloze.*[20] *Jejich metodiku neznám, ale vycházela z předpisů RBI. Obecně vzato, IT Risk Management byl ve sdílené gesci OIT a OŘR (primárně OIT), metodika analýzy IT rizik je popsána ve směrnicích RBI.*"[21]

24. Následně dne 10.11.2021 účastník řízení doplnil své vyjádření následovně: „*Dále doplním, že s převodem funkce security do RB (1.6.2021) jsme si převzali i povinnost provádět IT Risk Management (ITRM). Aktuálně na něm pracuje kolega. Analýza by měla být hotová do konce roku a nemyslím si, že by zatím byla v prezentovatelné podobě. Metodika vychází ze směrnic RBI (RBI Group IT Risk Management Framework). Skupinovou metodiku bychom měli implementovat do RSTS ve formě interního příkazu. Doplním, že za OpRisk jsme dodávali soubor IT_risk_points_2021.xlsx, který obsahoval všechna operační rizika na všech útvarech stavební spořitelny, identifikovaná v roce 2021 a související s IT.*"[22]

25. Účastník řízení dále dne 2.11.2021 zaslal správnímu orgánu následující soubory týkající se řízení aktiv IS/IT z hlediska bezpečnosti IS/IT: „*seznam_klasifikovanych_aplikaci PK.xlsx*", „*Risk analysis analyzia rizik rsts.xlsx*" a „*2020 Final RSTS RA OIT.xlsx*".[23]

26. Správní orgán přezkoumal předložené dokumenty a dospěl k závěru, že účastník řízení neprovedl komplexní analýzu bezpečnostních rizik spjatých s provozem IS/IT v rozsahu stanoveném Vyhláškou č. 163/2021 Sb.

---

[19] E-mail správního orgánu účastníkovi řízení ze dne 4.11.2021. Viz soubor „*Email_CNB_20211104*", spis, č. l. 5 (DVD).
[20] Viz soubor „*2020 Final RSTS RA OIT.xlsx*", spis, č. l. 5 (DVD).
[21] E-mail účastníka řízení správnímu orgánu ze dne 8.11.2021. Viz soubor „*Email_CNB_20211104.msg*", spis, č. l. 5 (DVD).
[22] E-mail účastníka řízení správnímu orgánu ze dne 10.11.2021. Viz soubor „*Email_RSTS_20211110.msg*", spis, č. l. 5 (DVD).
[23] Vše spis, č. l. 5 (DVD).

27. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[24] do 31.5.2021[25] neprováděl komplexní analýzu bezpečnostních rizik spjatých s provozem IS/IT, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení bodu 17 přílohy 6 vyhlášky č. 163/2014 Sb.**

ii) <u>Bezpečnostní monitoring</u>

28. Správní orgán v rámci Kontroly dále prověřoval systém bezpečnostního monitoringu účastníka řízení s ohledem na jeho velikost a význam, přičemž obsahem této části Kontroly bylo nastavení tvorby bezpečnostních auditních záznamů (dále jen „BAZ"), jejich sběru, ochrany a vyhodnocování za použití především SIEM[26] nástroje. Kontrola byla zaměřena především na proaktivní bezpečnostní monitoring a správní orgán prověřoval jeho účinnost.[27]

29. Dále vzal správní orgán do úvahy, že před zahájením Kontroly došlo k outsourcingu informační bezpečnosti účastníka řízení (tedy i procesu bezpečnostního monitoringu, který je nedílnou součástí) do RBCZ ode dne 1.6.2021,[28] a to včetně převodu technických nástrojů (především SIEM) a personálních kapacit. Vzhledem k tomu, že nastavení účinného a efektivního systému bezpečnostního monitoringu je poměrně dlouhodobý proces, správní orgán prověřoval úroveň tohoto procesu před provedením outsourcingu a také přihlédl ke stavu po provedení outsourcingu a převodu technických i personálních kapacit do RBCZ.

a) Efektivita procesu bezpečnostního monitoringu

30. Podle ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. povinná osoba zabezpečí, že proces rozpoznávání rizik je zajištěn u všech činností a na všech řídicích a organizačních úrovních a umožňuje odhalování nových, dosud neidentifikovaných rizik.

31. Při prověřování celkové úrovně procesu bezpečnostního monitoringu správní orgán identifikoval, že účastník řízení sice už před provedením outsourcingu nastavil základy takového procesu ve smyslu implementace SIEM nástroje, připojení některých zdrojů BAZ a do určité míry i jejich vyhodnocování, avšak celkový stav systému bezpečnostního monitoringu v době Kontroly shledal správní orgán **nedostatečně efektivním**. Správní orgán identifikoval následující dílčí nedostatky, které byly způsobilé snižovat účinnost celého systému, a to především v jejich vzájemné kombinaci.

---

[24] Počátek kontrolního období.

[25] Poslední den před provedením outsourcingu do RBCZ.

[26] Management bezpečnostních informací a událostí, z angl. *Security Information and Event Management*.

[27] Efektivní proaktivní bezpečnostní monitoring zajistí ve velkém množství událostí, které vznikají v IS/IT účastníka řízení, identifikaci a prioritizaci významných událostí indikujících potenciální škodlivé činnosti a narušení bezpečnosti IS/IT včetně včasné reakce na takové události s cílem minimalizovat škody a dopady na aktiva účastníka řízení. Z hlediska technické realizace se jedná především o automatizované kontroly tzv. usecases v nástroji typu SIEM, které zajistí vyhodnocování takových významných událostí v reálném čase (online) napříč všemi významnými systémy a dále korelaci souvisejících událostí napříč jednotlivými platformami IS/IT. Sledované události by měly být stanoveny na základě analýzy rizik a stanovena priorita takových kontrol vzhledem ke kapacitám a kritičnosti sledovaných událostí.

[28] Smlouva o poskytování služeb uzavřená mezi RBCZ a účastníkem řízení dne 31. 5. 2021. Viz soubory „*Smlouva o poskytování služeb CDR17927.pdf*" a „*Smlouva o poskytování služeb CDR17927 Zvláštní smlouva.pdf*", vše spis, č. l. 5 (DVD).

32. Účastník řízení uvádí v kapitole 2.1 předloženého pracovního pokynu *SIEM (management bezpečnostních informací a událostí)* (dále jen „PP SIEM“) následující požadavky na logování událostí ve svém IS/IT: *„Strategií OCOM není logovat všechno, co je možné (to by potenciálně vytvářelo velké objemy dat s velkým plýtváním), ale konkrétně a cíleně ty akce a činnosti, které jsou nezbytné při identifikaci potenciálních škodlivých činností tak, aby jim bylo možné v budoucnu zabránit, nebo alespoň prokázat jejich návaznost a identifikovat příčinu.“*[29] V této souvislosti byly v kapitole 3.1. *PP SIEM* stanoveny obecné požadavky na atributy BAZ (např. kdo vykonal určitou činnost, kdy, kde apod.) a typy BAZ napříč jednotlivými platformami IS/IT (např. přihlášení a odhlášení, použití privilegovaných účtů apod.). V Příloze č. 1 *PP SIEM* nazvané „*Zdrojové systémy pro Qradar*“ je pak uveden seznam na SIEM připojených zdrojových systémů bez podrobnější specifikace. Také v kapitole 6 vnitřního předpisu *Bezpečnostní politika informačních systémů a informačních technologií* jsou stanoveny obecné požadavky na typy BAZ napříč jednotlivými platformami IS/IT.[30]

33. Výše popsané obecné požadavky na atributy a především typy BAZ však nebyly v dostatečné míře rozpracovány ve formě **formálních a závazných požadavků na nastavení detailních auditních politik** na jednotlivých zdrojových systémech produkujících BAZ v rámci jednotlivých technologických platforem, jako jsou např. síťové prvky, operační systémy, databáze, aplikace apod. (rozsah, typy a atributy BAZ, požadavky na nastavení systémů a ochranu BAZ apod.).[31] Přitom nástroje typu SIEM a kontroly jimi prováděné jsou kriticky závislé na kvalitě a rozsahu načítaných BAZ. Účastník řízení tak nemá dostatečnou jistotu, že bude schopen naplnit výše uvedené požadavky v kapitole 2.1 *PP SIEM* týkající se především požadavku na vytváření pouze cílených a definovaných BAZ indikujících možné škodlivé činnosti v IS/IT účastníka řízení za účelem úspory zdrojů.

34. Správní orgán vzal do úvahy, že účastník řízení předložil instalační šablony a postupy týkající se určitých platforem (především operačních systémů),[32] ty však dostatečně nenaplňovaly výše uvedené požadavky ani z hlediska formálních a závazných postupů, ani z hlediska obsahu a především pokrytí všech používaných platforem. Dále, že v rámci RBCZ probíhal projekt „*CIS Hardening*“, který by měl v rámci outsourcingu informační bezpečnosti zajistit i pro účastníka řízení vypracování závazných pravidel a kontrolu shody, tento projekt však nebyl v době Kontroly pro účastníka řízení dostatečně implementován.

35. V době Kontroly nebyly na stávající SIEM připojeny, a tedy ani dostatečně proaktivně vyhodnocovány, BAZ z některých významných informačních systémů. Jednalo se

[29] Pracovní pokyn č. 05/2015 *SIEM (management bezpečnostních informací a událostí)*, verze č. 4, účinný od 21.9.2021. Viz Soubor „*PP 2015-05 SIEM management bezpečnostních informací a událostí V4.docx*“ spis, č. l. 5 (DVD).

[30] Příkaz č. 01/2012 Bezp*ečnostní politika informačních systémů a informačních technologií Raiffeisen stavební spořitelny a.s.*, verze č. 5. Viz soubor „*P 2012-01 Bezpečnostní politika IS, IT RSTS V5.docx*“, spis, č. l. 5 (DVD).

[31] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Potvrdit (především pan [redacted]), že RSTS nedisponovala a v současné době (po spuštění outsourcingu) nedisponuje závaznými požadavky (pravděpodobně v rámci závazných bezpečnostních konfiguračních standardů) na nastavení auditních politik na jednotlivých platformách…“* účastník řízení odpověděl (potvrdil aktuální stav): „*Vycházíme ze standardů RBI, respektujeme interní příkaz Bezpečnostní politika. **Ve větším detailu nejsme**, leda by něco stanovovaly předpisy pro řízení IT*.“ Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

[32] Viz soubor „*Instalace Win10 LTSC 64bit.pdf*“, spis, č. l. 5 (DVD).

především o BAZ na databázových systémech, Informix a MS SQL.[33] Přitom existovali uživatelé s přímým přístupem k databázím pod významnými aplikacemi, včetně většího množství uživatelů s administrátorskými oprávněními (cca 15) k databázi Informix kritické aplikace CIBIS.[34] Účastník řízení navíc nezajistil ani dostatečné auditní záznamy o činnosti takových uživatelů s přímým přístupem k databázi při používání SQL příkazů (čtení či případně modifikaci dat apod.)[35]

36. V předpisech skupiny RBI, především *RBI GROUP SECURITY MONITORING & THREAT INTEL STANDARD*, jsou stanoveny požadavky na bezpečnostní monitoring, včetně požadavku: „*SEM-001. Every IT change, initiative or project must start with a detailed analysis of required use cases, which means definition of log data (systems and events) and required reports. There must be a logging concept defined before starting implementation.*"[36] Tento požadavek však nebyl v době Kontroly dostatečně naplňován v praxi, jak potvrdil účastník řízení.[37]

37. **Nejvýznamnějším** nedostatkem v oblasti proaktivního bezpečnostního monitoringu účastníka řízení je pak jeho **nedostatečná efektivita**. Účastník řízení nezajistil v dostatečné míře detailní, formální a závazný popis kontrol ve formě aplikovaných

[33] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Potvrdit / okomentovat a uvést skutečnosti, že na SIEM Qradar nebyly / nejsou připojeny následující zdroje logů a nejsou ani proaktivně a online vyhodnocovány jiným způsobem: Databázové logy především Informix pod CIBIS, MS SQL apod.*" účastník řízení odpověděl (potvrdil aktuální stav): „***Potvrzuji**. Přesouvány do SIEM jsou pouze aplikační logy, které však nebyly vyhodnocovány – z toho důvodu je zavedena manuální měsíční kontrola nad kritickými transakcemi*." Viz soubor „*Dotazy_RSTS.docx*", spis, č. l. 5 (DVD).

[34] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*CIBIS - Potvrdit stav / okomentovat, že z předložených podkladů vyplývá (tabulka dbuzivatele.xls CIBIS Informix), že následující účty (celkově 15, minimálně 7 personálních) mají přímý přístup do DB Informix s plnými právy DBA – možnost číst i změnit jakákoliv data?*" účastník řízení odpověděl (potvrdil aktuální stav): „*Odpověď**: Ano je to tak. Mají přímý přístup***." Dále účastník řízení potvrdil přímé přístupy do databází i na úrovni aplikací SAP a ECM. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Dále dodat informaci, zda je vůbec činnost takového uživatele na příslušné DB logována (auditní politika) – provádění SQL příkazů jak pasivních SELECT tak aktivních INSERT, UPDATE, DELETE apod.*" účastník řízení odpověděl (potvrdil aktuální stav): „***Audit SQL příkazů není aktivní***." Viz soubor „*Dotazy_RSTS.docx*", spis, č. l. 5 (DVD).

[35] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*CIBIS - Potvrdit stav / okomentovat, že z předložených podkladů vyplývá (tabulka dbuzivatele.xls CIBIS Informix), že následující účty (celkově 15, minimálně 7 personálních) mají přímý přístup do DB Informix s plnými právy DBA – možnost číst i změnit jakákoliv data?* " účastník řízení odpověděl (potvrdil aktuální stav): „*Odpověď**: Ano je to tak. Mají přímý přístup***." Dále účastník řízení potvrdil přímé přístupy do databází i na úrovni aplikací SAP a ECM - na dotaz správního orgánu (žádost o potvrzení stavu): „*Dále dodat informaci, zda je vůbec činnost takového uživatele na příslušné DB logována (auditní politika) – provádění SQL příkazů jak pasivních SELECT tak aktivních INSERT, UPDATE, DELETE apod.*" účastník řízení odpověděl (potvrdil aktuální stav): „***Audit SQL příkazů není aktivní***." Viz soubor „*Dotazy_RSTS.docx*", spis, č. l. 5 (DVD).

[36] Supporting Document to Internal Reg RBI Group Information & Cyber Security Policy. Viz soubor „*SUP-2018-0159_RBI Group Security Monitoring & Threat Intel Standard_V1.4.pdf*", spis, č. l. 5 (DVD).

[37] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Potvrdit / okomentovat, že RSTS dostatečně nesplňovala a ani nesplňuje požadavky na bezpečnostní monitoring v závazném? Předpise RBI SUP RBI Group Security Monitoring & Threat Intel Standard V1.2*" účastník řízení odpověděl (potvrdil aktuální stav) pro požadavek a) SEM-001: „***Potvrzuji,** jedná se o jeden z **nedostatků evidovaných v SCA**. Koncept logování na systémové úrovni měl být vytvořen ze strany OIT do 03/2021. Na aplikační úrovni jsou use-cases součástí dokumentace, ale neexistuje žádný check-list, který by nařizoval, aby use-cases braly v potaz logování.*" Viz soubor „*Dotazy_RSTS.docx*", spis, č. l. 5 (DVD).

usecases (pravidel) na SIEM nástroji.[38,39] Spoléhal se především na defaultní pravidla (usecases) v SIEM nástroji, ty však nebyl vždy schopen dostatečně adaptovat a validovat s ohledem na specifické podmínky svého prostředí. Přitom se jednalo o usecases (pravidla), která mají zachycovat, analyzovat a proaktivně vyhodnocovat události požadované výše uvedeným skupinovým předpisem *RBI GROUP SECURITY MONITORING & THREAT INTEL STANDARD*.[40] Jednalo se např. o požadavek na detekci a analýzu událostí v usecases „*Detection of possible Brute Force Attacks, Malicious administrator activities, Misuse of privileged access, Malicious user behaviour (DLP), Log collector compromised, Malicious administrator activities, Unauthorized access to log collector, Compromised logging source, Destruction of evidence*“ apod. Na dotaz správního orgánu, zda účastník řízení dodržuje tyto požadavky, odpověděl účastník řízení následovně: *„Tyto scénáře jsou součástí defaultních QRadar pravidel.* ***Nemůžu ale potvrdit, že jsou nasazeny správně****, mé snahy o zvýšení oprávnění neprošly přes pana* [redacted]*,* ***validace těchto pravidel neproběhla****. Na této aktivitě pracujeme v RB ve spolupráci s externím specialistou*“ (zdůrazněno správním orgánem).[41]

38. Správní orgán vzal do úvahy, že účastník řízení zpracoval popis kontrol, týkající se především tzv. „*kritických transakcí a privilegovaných účtů*“. Tyto kontroly se však prováděly převážně „ručně“, mimo SIEM nástroj přímo nad BAZ kritické aplikace CIBIS (z důvodu technických problémů s načítáním BAZ z aplikace do SIEM) a nebyly prováděny online, zpravidla pouze 1x měsíčně.[42] Účastník řízení tak neměl dostatečnou jistotu, že je schopen vyhodnotit celkovou úroveň a efektivitu procesu bezpečnostního monitoringu a zajistit i jeho zdokonalování, a dále, že systém proaktivního bezpečnostního monitoringu dokáže dostatečně identifikovat a prioritizovat významné události indikující potenciální škodlivé činnosti a narušení bezpečnosti IS/IT, a reagovat na ně včas s cílem minimalizovat škody a dopady na aktiva účastníka řízení.

39. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[43] do 31.5.2021[44] nezajistil identifikaci a prioritizaci významných událostí indikujících potenciální hrozby a narušení systému IS/IT, včetně včasné reakce s cílem minimalizovat škody, čímž se vystavoval riziku neodhalení či pozdního odhalení škodlivých činností v jeho informačních systémech, čímž postupoval**

[38] Včetně např. popisu sledovaných platforem a událostí, formy a četnosti zpracování, odpovědností a procesů L1,2,3, komunikace s ostatními útvary především IT, kritérií pro vyhodnocení false positive versus incident, checklistu takových kontrol (denní rutina) apod.

[39] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Existuje? Podrobnější popis kontrol (usecases) jako knowledge base – proaktivní monitoring prováděných v SIEM Qradar na připojených zdrojích v RSTS před outsourcingem …* “ účastník řízení odpověděl (potvrdil aktuální stav): „*Security Officer postupoval dle pracovního pokynu č. 05/2015 SIEM, vytvářel Excel k provedeným kontrolám, přikládám zde, kontroly byly prováděny na týdenní až měsíční bázi a reportovány kvartálně na výborech ORCO. Komunikace s IT útvarem a se zaměstnanci probíhala ad-hoc dle potřeby, přes maily, na výborech apod.,* ***Use-cases, jaké píšete výše, nebyly formálně stanoveny****.*“ Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

[40] Supporting Document to Internal Reg RBI Group Information & Cyber Security Policy. Viz soubor „*SUP-2018-0159_RBI Group Security Monitoring & Threat Intel Standard_V1.4.pdf*“, spis, č. l. 5 (DVD).

[41] Odpověď účastníka řízení zaslaná v rámci e-mailové komunikace se správním orgánem dne 25.11.2021. Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

[42] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Frekvence kontrol byla buď 1x měsíc / půl roku, častější (online) nebyly?*“ účastník řízení odpověděl (potvrdil aktuální stav): „*Frekvence byla* ***max 1x / měsíc*** *s kvartálním reportingem na ORCO, online vyhodnocovány* ***nebyly****.*“ Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

[43] Počátek kontrolního období.

[44] Poslední den před provedením outsourcingu do RBCZ.

v rozporu s požadavkem upřesněným v ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb.

b) Funkčnost SIEM nástroje

40. Podle ustanovení bodu 16 přílohy č. 6 k vyhlášce č. 163/2014 Sb. povinná osoba zajistí dodržování bezpečnostních zásad v jednotlivých informačních systémech.

41. Správní orgán v rámci Kontroly zjistil nedostatky, které se týkaly i samotné **funkčnosti** SIEM nástroje, a tedy i efektivity procesu bezpečnostního monitoringu. Účastník řízení reportoval incident spojený s výpadkem SIEM nástroje: „*SIEM system IBM QRadar did not log data between 27/04/2020 until 20/05/2020. The outage was discovered by an Information Security Officer during monthly review. The problem was repaired right after discovery. During the outage there was no supplementary solution implemented.*“[45] Z popisu tohoto incidentu a dalších dodaných materiálů vyplývá, že jednak **kompletní výpadek tohoto nástroje trval téměř měsíc, a v průběhu této doby nenačítal ani nevyhodnocoval BAZ, a jednak, že tento stav nebyl identifikován včas bez zbytečné prodlevy.**[46,47]

42. Účastník řízení vyhodnotil tento incident pouze s nejnižší prioritou („*LOW*“) s následujícím zdůvodněním: „*Historicky se v Qradaru nacházely neprioritní incidenty. V Qradaru nikdy nebyl zaznamenán incident, který by vyžadoval prioritní řešení*.“[48] Účastník řízení dále potvrdil, že i v průběhu roku 2021 (tj. i po outsourcingu bezpečnostního monitoringu do RBCZ) docházelo k významným a dlouhodobým výpadkům funkčnosti SIEM nástroje, a tedy i procesu proaktivního bezpečnostního monitoringu. Tyto skutečnosti byly projednávány i na Výboru pro bezpečnost účastníka řízení dne 26.8.2021, kde bylo konstatováno následující: *„The Committee discussed gaps in log monitoring. The system used to collect logs from various sources in RSTS is QRadar, which is **not functioning due to expired licenses**. A replacement **is not** yet prepared.*“ A dále: „*Due to a **lack of log collection and evaluation**, RSTS is not fully compliant with Cyber act and RBI group standards. The Committee agreed that Log monitoring is a crucial*“ (zdůrazněno správním orgánem).[49]

43. Na dotaz správního orgánu k těmto výpadkům: „*Dle vyjádření HO Information Security RB na schůzce získali přístup do SIEM až v 10/2021, do té doby neměli visibilitu – okomentovat, do té doby SIEM nefungoval? Nebo se s ním nepracovalo?*“ účastník řízení

[45] Nahlášení incidentu ze dne 5.6.2020. Viz soubor „*SIEM_incident.pdf*“, spis, č. l. 5 (DVD).

[46] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „ *Bližší popis výpadku, SIEM vůbec nepracoval ve smyslu načítání / vyhodnocování logů?*“ účastník řízení odpověděl (potvrdil aktuální stav): „***Ano**, v této době byl server spadlý, **nenačítal ani nevyhodnocoval logy***“. Dále na dotaz správního orgánu (žádost o potvrzení stavu) „ *Bližší popis jak pan [redacted] tento stav objevil, znamená to, že se SIEM nepracoval online ale pouze na měsíční bázi – připojil se do konzole 1 x měsíc, či v delší časové periodě?* “ účastník řízení odpověděl (potvrdil aktuální stav): „*QRadar běžel neustále (pokud neměl výpadek), **Ano**, kontroly ze strany Security Officera probíhaly na **týdenní až měsíční bázi**, kvartálně byly reportovány na ORCO.*“ Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

[47] Taktéž v reportu incidentu ze dne 5.6.2020 účastník řízení zaznamenal dobu trvání incidentu („*Event Duration*“) 23 dní a dobu odhalení incidentu („*Discovery time Duration*“) 39 dní. Viz soubor „*SIEM_incident.pdf*“, spis, č. l. 5 (DVD).

[48] Odpověď účastníka řízení zaslaná v rámci e-mailové komunikace se správním orgánem dne 25.11.2021. Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

[49] Zápis z jednání Výboru pro bezpečnost účastníka řízení ze dne 26.8.2021. Viz Soubor „*L-SC_RSTS_Meeting_Minutes_2021_08_26_v1.docx*“, spis, č. l. 5 (DVD).

uvedl: *„SIEM **měl výpadek, údajně vypršely licence = nefungoval., nelogoval, nevyhodnocoval**. Toto bylo reportováno na výborech ORCO,*“ a dále „*V průběhu února 2021 **nastal výpadek logů** z QRadaru, logy se nepodařilo během 1Q ani 2Q 2021 obnovit. Za 2021 nebyly statistiky zpracovány, **protože systém neběžel**. Na LSC RSTS 3Q bylo toto definováno jako prioritní záležitost*“ (zdůrazněno správním orgánem).[50]

44. Z výše uvedených skutečností vyplývá, že **nebyla dostatečně zajištěna ani samotná funkčnost klíčového SIEM nástroje, ani proaktivní kontrolní činnost umožňující bez zbytečného prodlení identifikovat jeho výpadek a přijmout nápravná opatření.** Z důvodu výpadku SIEM nástroje a obecně i tvorby a vyhodnocování BAZ pak účastník řízení nebyl schopen dostatečně analyzovat příčiny či případnou škodlivou činnost útočníka v rámci reálného incidentu týkajícího se nákazy malware (blíže viz odst. 53 a násl. tohoto příkazu)**Chyba! Nenalezen zdroj odkazů.**.

45. Ve světle výše uvedeného správní orgán konstatuje, že účastník řízení **nezavedl dostatečně efektivní systém proaktivního bezpečnostního monitoringu,** především ve vztahu k identifikaci a prioritizaci významných událostí indikujících potenciální škodlivé činnosti a narušení bezpečnosti IS/IT, včetně včasné reakce na takové události s cílem minimalizovat škody a dopady na aktiva účastníka řízení. Tím se účastník řízení vystavoval riziku neodhalení, či pozdního odhalení škodlivých činností v jeho informačních systémech.

46. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 27.4.2020[51] do 6.9.2021[52] nezajistil funkčnost SIEM nástroje IBM QRadar, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení bodu 16 přílohy č. 6 k vyhlášce č. 163/2014 Sb.**

iii) <u>Ochrana proti pokročilým kybernetickým hrozbám</u>

47. Podle ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. povinná osoba zabezpečí, že proces rozpoznávání rizik je zajištěn u všech činností a na všech řídicích a organizačních úrovních a umožňuje odhalování nových, dosud neidentifikovaných rizik.

48. Podle bodu 36 písm. d) Obecných pokynů EBA/GL/2019/04 by finanční instituce měly zavést postupy, které zabrání výskytu bezpečnostních incidentů v systémech IKT [informační a komunikační technologie] a službách v oblasti IKT, a měly by minimalizovat jejich dopad na poskytování služeb v oblasti IKT. Tyto postupy by měly zahrnovat minimálně opatření na zavedení ochrany koncových bodů včetně serverů, pracovních stanic a mobilních zařízení; finanční instituce by měly vyhodnotit, zda koncové body splňují jimi vymezené bezpečnostní standardy, než bude těmto bodům umožněn přístup do podnikové sítě.

49. Podle bodu 60 písm. d) a e) Obecných pokynů EBA/GL/2019/04 by finanční instituce měly stanovit vhodné postupy a organizační struktury, které zajistí jednotné a integrované sledování, řešení a návazné sledování provozních a bezpečnostních incidentů a zabezpečí, aby byly identifikovány a odstraněny hlavní příčiny a předešlo se výskytu opakovaných

[50]Odpověď účastníka řízení zaslaná v rámci e-mailové komunikace se správním orgánem dne 25.11.2021. Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).
[51] Datum prvního zaznamenaného výpadku SIEM systému.
[52] Konec kontrolního období dle Protokolu.

incidentů. Postup řízení incidentů a problémů by měl stanovit požadavky na účinné a efektivní plány interní komunikace významných incidentů a efektivní *incident response* procedury minimalizující dopady významných incidentů a útoků.

50. Správní orgán s ohledem na velikost a význam účastníka řízení prověřoval úroveň a efektivitu systému řízení nových a dosud neidentifikovaných rizik v oblasti pokročilých kybernetických hrozeb, např. APT útoků.[53] Dále vzal do úvahy, že před zahájením Kontroly došlo k outsourcingu informační bezpečnosti účastníka řízení (zahrnujícího i proces ochrany proti pokročilým kybernetickým hrozbám) do RBCZ (skupiny RBI) ode dne 1.6.2021,[54] a to včetně převodu technických nástrojů a personálních kapacit a implementace nových společných technických nástrojů. Vzhledem k tomu, že nastavení účinného a efektivního systému ochrany proti pokročilým kybernetickým hrozbám je poměrně dlouhodobý proces, správní orgán prověřoval úroveň tohoto procesu už před provedením outsourcingu a také přihlédl ke stavu po provedení outsourcingu a převodu technických i personálních kapacit do RBCZ (skupiny RBI).

51. Při prověřování celkové úrovně procesu ochrany proti pokročilým kybernetickým hrozbám správní orgán identifikoval **zásadní nedostatky** v oblasti systematické a proaktivní kontroly v této oblasti. Všechny níže uvedené nedostatky, včetně reálného významného incidentu v oblasti malware a závažných zranitelností identifikovaných v provedených penetračních testech, poukazují na **nedostatečnou úroveň řízení rizik v oblasti pokročilých kybernetických hrozeb. Kombinace těchto nedostatků zvyšuje riziko úspěšného sofistikovaného kybernetického útoku na účastníka řízení bez dostatečně včasné a rychlé identifikace IOC, reakce na tento útok a spuštění incident response procesu s cílem co nejvíce zmírnit dopady takového útoku.**

52. Správní orgán pro úplnost konstatuje, že uvedené zjištění se vztahuje pouze ke kontrolnímu období a týká se především úrovně řízení rizik **před provedením outsourcingu** do RBCZ (skupiny RBI). Správní orgán identifikoval určité náznaky zlepšení tohoto stavu po převodu procesu ochrany proti pokročilým kybernetickým hrozbám do RBCZ v rámci outsourcingu, týkající se např. probíhající implementace lepší ochrany koncových bodů (ALEF Octoshield a použití EDR nástroje CISCO AMP) a dalších služeb a technických nástrojů např. na společném perimetru mj. i jako reakci na níže popsaný incident.

a) Hlášení bezpečnostního incidentu

53. Účastník řízení reportoval na NÚKIB kybernetický bezpečnostní incident týkající se nálezu škodlivého kódu (malware) na významném technologickém serveru - doménovém řadiči (tedy řídícím serveru celé Windows domény).[55] V hlášení incidentu účastník řízení mj. uvedl, že „[m]*alware se potvrdil na doménovém řadiči DC11 – jeden ze dvou hlavních*

[53] Efektivní systém řízení nových a neidentifikovaných rizik v oblasti pokročilých kybernetických hrozeb zahrnuje systematickou a proaktivní kontrolní činnost za pomoci vhodných technických nástrojů. Ty jsou založeny jak na tradiční obraně sítě (antivir, FW apod.), tak na pokročilejších nástrojích (např. EDR, IDS/IPS, SIEM apod.), které vhodně doplňují tradiční obranu sítě. Jsou tak schopny včas identifikovat jednotlivé IOC. Nedílnou součástí takového systému jsou také preventivní či reaktivní procesy, které doplní tyto kontroly a minimalizují tak dopady na aktiva oběti útoku.

[54] Smlouva o poskytování služeb uzavřená mezi RBCZ a účastníkem řízení dne 31. 5. 2021. Viz soubory „*Smlouva o poskytování služeb CDR17927.pdf*“ a „*Smlouva o poskytování služeb CDR17927 Zvláštní smlouva.pdf*“, vše spis, č. l. 5 (DVD).

[55] Formulář hlášení kybernetického bezpečnostního incidentu ze dne 15.10.2021. Viz soubor „*RSTS_Formular_incident_report_govcert_NUKIB.pdf*“, spis, č. l. 5 (DVD).

doménových řadičů v RSTS. Předpokládá se kompromitace celé domény." Správní orgán zjistil, že na dotyčném serveru **nebyla nainstalována** odpovídající pokročilá antivirová ochrana a administrátor účastníka řízení objevil malware náhodou při rutinní činnosti, což vyplývá i z hlášení incidentu: *„*[a]*dministrátor RSTS, při rutinní činnosti (vytváření uživatelů), připojil disk serveru jako síťový disk do své pracovní stanice, aby na něj nakopíroval skripty, které se následně chystal spustit. Na připojení reagoval antivirus, který začal nově připojený disk skenovat. Při skenování nalezl malware, klasifikovaný jako: VirTool:Win32/RemoteExec. Později se zjistilo, že server, na kterém byl malware nalezen, je doménový kontroler*."[56]

54. V rámci hlášení incidentu účastník řízení dále uvedl: *„Datum a čas výskytu incidentu: 21. 6. 2021*" a „*Datum a čas zjištění incidentu: 15. 10. 2021*", z čehož vyplývá, že **incident byl identifikován se zpožděním minimálně téměř 4 měsíce**. Z uvedených informací vyplývá, že **účastník řízení nenastavil dostatečnou úroveň systematické a proaktivní kontrolní činnosti za použití vhodných technických nástrojů, která by zajistila identifikaci škodlivých činností (IOC) v IS/IT dostatečně včas a bez zbytečné prodlevy tak, aby byly minimalizovány dopady na účastníka řízení.**

55. Předložená závěrečná zpráva k tomuto incidentu dále konstatuje: *„*[p]*oměrně brzy po prvotní detekci jsme byli schopni zjistit, že malware se na serverech nachází od 21. 6. 2021, což jsou téměř čtyři měsíce, než jsme malware detekovali a získali obrazy disků pro forenzní analýzu. Bylo již vcelku jasné, že z disků samotných už moc informací nezískáme, protože téměř všechny forenzní artefakty jsou v tuto chvíli přepsány. Protože v době, kdy k incidentu došlo**, *nebyl funkční SIEM** (nástroj pro shromažďování a analýzu logů), chybí nám klíčové podklady, jako jsou systémové logy a logy síťového provozu, bez nichž zkrátka nelze odhalit, co se na systému přesně stalo, a hlavně kdo a odkud k systému pod uživatelem administrator přistupoval*" (zdůrazněno správním orgánem).[57] Z této zprávy vyplývá, že účastník řízení z důvodu **nefunkčnosti SIEM nástroje (a tedy i procesu bezpečnostního monitoringu)** a zpoždění při detekci incidentu **nebyl dostatečně schopen ani zpětně ad hoc analyzovat příčiny incidentu a identifikovat možné IOC**.[58] Sám účastník řízení přitom ve výše uvedené zprávě uvádí identifikované nedostatky z tohoto incidentu jako *„nefunkční provozní / bezpečnostní monitoring*", „*absence pokročilé antivirové ochrany na serverech*" apod.

56. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 21.6.2021[59] do 15.10.2021[60] nenastavil dostatečnou úroveň systematické a proaktivní kontrolní činnosti za použití vhodných technických nástrojů, která by zajistila identifikaci škodlivých činností v IS/IT včas tak, aby byly minimalizovány dopady, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. ve spojení s bodem 36 písm. d) Obecných pokynů EBA/GL/2019/04.**

---

[56] Tamtéž.

[57] Závěrečná zpráva k Incidentu číslo INC-13538 ze dne 15.11.2021. Viz soubor „*RSTS_Zaverecna_zprava_k_INC_20211115.pdf*", spis, č. l. 5 (DVD).

[58] Např., že nedošlo k nějaké další škodlivé činnosti, neautorizované komunikaci v rámci sítě či do internetu, pokusům (úspěšným či neúspěšným) o škodlivou činnost např. ve smyslu krádeže citlivých dat, další nákazy malware apod., která by byla zaznamenána v příslušných BAZ

[59] Datum výskytu bezpečnostního incidentu.

[60] Datum odhalení bezpečnostního incidentu.

b) Výsledky penetračních testů

57. Výše uvedené nedostatky v systému řízení rizik pokročilých kybernetických hrozeb byly ještě umocněny dalšími dílčími nedostatky zjištěnými správním orgánem v rámci Kontroly. Účastník řízení předložil dokument „*Penetrační testy infrastruktury RSTS*“.[61] Z výsledků penetračních testů vyplynuly závažné nedostatky a zranitelnosti v síti účastníka řízení. Minimálně 9 nálezů bylo označeno jako „*kritické*“, tzn. umožňující útočníkovi převzít kontrolu nad servery, administrátorskými účty domény Windows apod.

58. **Z nálezu penetračních testů mj. vyplývá, že nebyla dostatečně aplikována bezpečnostní opatření týkající se aplikace bezpečnostních záplat a byly provozovány nezabezpečené a staré verze systémů, nebyla dostatečně aplikována opatření týkající se bezpečné autentizace privilegovaných účtů (slabá a sdílená hesla apod.) a další.**

59. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 21.6.2021[62] do 22.7.2021[63] nenastavil dostatečnou úroveň systematické a proaktivní kontrolní činnosti, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb.**

c) Incident Response plány

60. Dále správní orgán požadoval[64] předložení *incident response* plánů pro jednotlivé typy významných útoků typu DDoS, APT, Phishing, rozsáhlá nákaza ransomware apod., které by reflektovaly specifika takových útoků. Účastník řízení takové plány předložil.[65] **Tyto plány však nebyly v době Kontroly dostatečně aktuální.** Byla zde uvedena jména osob, které u účastníka řízení či RBCZ v době Kontroly již nepracovaly, byly uvedeny neaktuální názvy útvarů, po obsahové stránce plány dostatečně nereflektovaly změny týkající se outsourcingu informační bezpečnosti do RBCZ, např. používání nových společných technických nástrojů na perimetru i koncových bodech (např. služba ALEF Octoshield a použití EDR nástroje CISCO AMP při identifikaci malware, služby typu ZEROFOX apod.). Jak dále uvedl účastník řízení v odpovědi na dotaz správního orgánu, **nebyly zpracovány incident response plány pro všechny požadované významné typy útoků.** Např. nebyl zpracován plán pro rozsáhlou nákazu ransomware či APT útok, se specifiky takového typu útoku, a stávající plány tak neobsahovaly všechny potřebné postupy.[66]

---

[61] Výsledná zpráva z penetračních testů infrastruktury ze dne 22.7.2021. Viz soubor „*AEC_PT_RBCZ_Infrastruktura_RSTS_report_v2.pdf*“, spis, č. l. 5 (DVD).

[62] Datum počátku testování interní infrastruktury.

[63] Datum konce testování externí infrastruktury.

[64] Výzva správního orgánu ze dne 3.9.2021, č. j. 2021/091687/CNB/580, bod A14. Viz soubor „*2021_091687_CNB_580_RSTS_Oznameni_o_zahajeni_kontroly_vyzva_a_pouceni.pdf*“, spis, č. l. 5 (DVD).

[65] Pohotovostní plány účastníka řízení pro jednotlivé typy významných útoků. Viz soubory „*Pohotovostní plán pro DDoS útok na www.rsts.cz.docx*“, „*Pohotovostní plán pro malware útok.docx*“ a „*Pohotovostní plán pro spoofing útok na www.rsts.cz.docx*“, spis, č. l. 5 (DVD).

[66] Účastník řízení potvrdil tento stav v rámci e-mailové komunikace se správním orgánem. Na dotaz správního orgánu (žádost o potvrzení stavu): „*Potvrdit, že předložené incident response nejsou aktuální a tudíž neodráží dostatečně efektivní incident response proces. Dále že tyto plány nepokrývají specificky oblast ransomware a APT hrozeb a že nebyly dostatečně otestovány alespoň od stolu“,* účastník řízení odpověděl (potvrdil aktuální stav): „*Plány **přestaly být aktuální** s odchodem angažovaných osob. Obsahově jsou podle mě relevantní, popisují response plán tak, jak by byl spuštěn v případě výskytu incidentu. Plány měly být dále doplněny o kroky na straně OIT, **k čemuž však nedošlo**. **Potvrzuji, že response plány nepokrývají ransomware ani APT a nebyly otestovány (byť byly vytvořeny na základě incidentu)***“. Viz soubor „*Dotazy_RSTS.docx*“, spis, č. l. 5 (DVD).

61. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 30.6.2020[67] do 31.8.2021[68] nezavedl efektivní incident response procedury minimalizující dopady významných incidentů a útoků, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. ve spojení s bodem 36 písm. d) Obecných pokynů EBA/GL/2019/04 a bodem 60 písm. d) a e) Obecných pokynů EBA/GL/2019/04.**

iv) <u>Provoz IS/IT</u>

a) Nepodporované informační systémy a nezabezpečené protokoly

62. Podle ustanovení § 23 odst. 5 písm. c) vyhlášky č. 163/2014 Sb. povinná osoba zabezpečuje ochranu informačních a komunikačních systémů před přístupem a zásahy ze strany neoprávněných osob a před poškozením a možnost zpětně získat stanovené informace i v případě, že k poškození došlo.

63. Podle ustanovení § 27 odst. 1 písm. d) vyhlášky č. 163/2014 Sb. povinná osoba při řízení rizik zohledňuje všechna významná rizika a rizikové faktory, kterým je nebo může být vystavena s přihlédnutím k povaze, rozsahu a složitosti činností. Řízení rizik v jeho celku i částech zohledňuje vnitřní a vnější faktory včetně zohledňování budoucí strategie podnikání povinné osoby, vlivů ekonomického prostředí a cyklu a vlivů regulatorního prostředí. Řízení rizik zohledňuje kvantitativní a kvalitativní aspekty rizik, reálné možnosti jejich řízení a náklady a výnosy vyplývající z řízení rizik.

64. Účastník řízení dle exportu z konfigurační databáze[69] provozoval v interní síti servery a stanice, jejichž operační systémy již nebyly výrobcem podporovány a jejich provoz představoval vzhledem k absenci bezpečnostních záplat riziko chyb a zneužití zranitelností na těchto serverech. Jednalo se o 8 serverů Windows 2003 Standard, 6 stanic s Windows 7 nebo 24 serverů Windows 2008 R2 Standard, mezi nimiž byly i řadiče domény Active Directory, tzn. jeden z klíčových informačních systémů účastníka řízení. Přítomnost nepodporovaných či zranitelných informačních systémů v interní síti účastníka řízení byla identifikována také v průběhu penetračního testu infrastruktury v červnu 2021[70] a v dokumentu společnosti Alef 0 popisujícím doménu účastníka řízení.[71]

65. **Ukončení podpory systému mj. znamená, že výrobce již neodstraňuje chyby softwaru a nevydává bezpečnostní záplaty pro nově objevené zranitelnosti.** Ukončení podpory pro operační systém Windows Server 2003 nastal v červenci 2015, pro Windows 7 a Windows 2008 v lednu 2020. **Účastník řízení neměl nastaven proces, který by monitoroval konec podpory jednotlivých platforem, přičemž migrační aktivity by měly být ukončeny ještě před vypršením platnosti garantované podpory výrobce.**

66. Účastník řízení dále používal **nezabezpečené protokoly pro komunikaci mezi informačními systémy ve vnitřní síti.** Absence šifrování komunikace v prostředí účastníka řízení byla např. zmíněna v bodě 9 zápisu z 1. jednání Výboru pro bezpečnost ze dne 13. 5. 2021:„*ve vnitřní síti RSTS neprobíhá šifrování komunikace, a to z kapacitních důvodů. Zavedení šifrování bude vyžadovat i technologickou změnu systému.*

[67] Datum účinnosti Obecných pokynů EBA/GL/2019/04
[68] Poslední den před provedením outsourcingu do RBCZ.
[69] Viz soubor „*Copy of CMDB_RSTS_ITOP.xlsx*“, záložka „*pocty*“, spis, č. l. 5 (DVD).
[70] Viz soubor „*AEC_PT_RBCZ_Infrastruktura_RSTS_report_v2.pdf*“, spis, č. l. 5 (DVD).
[71] Viz soubor „*AD-RSTS.docx*“, spis, č. l. 5 (DVD).

Téma bude řešeno až po integraci s RBCZ.“ [72] Z uvedeného vyplývá riziko tzv. Man in the Middle útoku, kdy se útočník ve vnitřní síti dostane mezi obě komunikující strany a může tak odposlouchávat veškerou nešifrovanou komunikaci, která může obsahovat osobní údaje, hesla a jiné důvěrné informace.

67. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[73] do 31.8.2021[74] provozoval v interní síti servery a stanice, jejichž operační systémy již nebyly výrobcem podporovány a jejich provoz tak představoval riziko chyb a zneužití zranitelností plynoucí z absence bezpečnostních záplat, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 23 odst. 5 písm. c) a § 27 odst. 1 písm. d) vyhlášky č. 163/2014 Sb.**

b) Hardening a kontrola shody

68. Podle bodu 21 písm. e) přílohy č. 6 k vyhlášce č. 163/2014 Sb. při provozování informačních systémů povinná osoba zejména zajistí pravidelné prověřování a vyhodnocování bezpečnosti informačních systémů.

69. V době Kontroly účastník řízení neměl ucelené formalizované bezpečnostní požadavky pro jednotlivé informační systémy jako např. Windows 10 na pracovních stanicích uživatelů, Windows server a RedHat Linux na serverech, databáze Informix a MS SQL. Účastník řízení se ohledně definice požadavků nacházel v přechodném stavu. Byly doloženy dokumenty, podle nichž se účastník řízení zabýval výběrem bezpečnostních benchmarků pro některé informační systémy založené na platformě CIS (Center for Internet Security)[75]. Z předložených dokumentů však nebyl zřejmý rozsah platnosti požadavků, tj. které parametry budou pro jednotlivé informační systémy účastníka řízení závazné a které nikoliv, způsob nastavení a kontroly parametrů a řízení výjimek ze standardu. Dále byly předloženy blíže nespecifikované testy souladu s CIS standardy pro server RedHat Enterprise Linux 7 a stanici s Windows 10[76,77] a instalační dokumentace pro Windows 10[78]. Tyto podklady však neobsahovaly požadavky na bezpečnost systémů definované účastníkem řízení.

70. Vzhledem k absenci schválených bezpečnostních požadavků účastník řízení nemohl provádět účinnou kontrolu reálného nastavení bezpečnostních parametrů informačních systémů a vystavoval se tímto zranitelnostem, které by mohly být odhaleny funkčním procesem kontroly shody s bezpečnostními požadavky. Účastník řízení též neměl dostatečné ujištění, že v provozovaných systémech nedocházelo v průběhu jejich životního cyklu k neautorizovaným změnám.

71. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[79] do 31.8.2021[80] neměl ucelené formalizované bezpečnostní**

[72] Viz soubor „*Zápis z jednání 20210513.docx*“, spis, č. l. 5 (DVD).
[73] Počátek kontrolního období.
[74] Poslední den před provedením outsourcingu do RBCZ.
[75] Viz jednotlivé soubory ve složce „*CIS Hardening*“ předané správnímu orgánu dne 11.11.2021, které obsahovaly výčet parametrů pro systémy Windows 10, RedHat Enterprise Linux 7, AIX, Solaris, spis, č. l. 5 (DVD).
[76] Viz soubor „*SERVERS-CIS_Red_Hat_Enterprise_Linux_7_Benchmark.html*“, spis, č. l. 5 (DVD).
[77] Viz soubor „*ENDPOINTS-CIS_Microsoft_Windows_10_Enterprise_Release_20H2_Benchmark.html*“, spis, č. l. 5 (DVD).
[78] Viz soubor „*Instalace Win10 LTSC 64bit.pdf*“, spis, č. l. 5 (DVD).
[79] Počátek kontrolního období.
[80] Poslední den před provedením outsourcingu do RBCZ.

požadavky pro jednotlivé jím používané informační systémy, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení bodu 21 písm. e) přílohy č. 6 k vyhlášce č. 163/2014 Sb.

c) Prevence úniku dat

72. Podle ustanovení § 27 odst. 1 písm. d) vyhlášky č. 163/2014 Sb. povinná osoba při řízení rizik zohledňuje všechna významná rizika a rizikové faktory, kterým je nebo může být vystavena s přihlédnutím k povaze, rozsahu a složitosti činností.

73. Účastník řízení nepoužíval v době Kontroly **žádný systematický nástroj pro detekci nebo prevenci úniku dat.** Zavedl pouze dílčí opatření ve formě omezení používání USB úložišť nástrojem Symantec Endpoint Protection a odepření přístupu na webová úložiště nastavením blacklistu na proxy serveru. **Další kanály možného úniku dat jako např. e-mailová komunikace, nešifrovaná zálohovaná data nebo tisky dokumentů účastník řízení systematicky neošetřil.**

74. Dále např. síťový provoz a síťové disky účastníka řízení nebyly monitorovány za účelem detekce možných úniků dat. Účastník řízení vykazoval vzhledem k velkému množství klientů a spravovaných důvěrných dat vyšší riziko právě v oblasti narušení důvěrnosti dat a z toho vyplývající ztráty reputace banky. K vyššímu riziku přispíval i účastníkem řízení detekovaný vyšší výskyt phishingu na klienty i zaměstnance v roce 2021[81] a další identifikované nedostatky v oblasti bezpečnosti informačních systémů.

75. V oblasti prevence úniku dat zavedl účastník řízení dílčí opatření, která nedostatečně pokrývala všechny směry možných úniků dat. Také vzhledem k absenci strategie či analýzy této oblasti nelze prevenci či ochranu proti únikům dat označit za systematickou. Z toho vyplývalo riziko úniku důvěrných, např. klientských dat účastníka řízení.

76. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[82] do 31.8.2021[83] nepožíval systematický nástroj pro detekci a prevenci úniku dat, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 27 odst. 1 písm. d) vyhlášky č. 163/2014 Sb.**

v) <u>Elektronické bankovnictví</u>

a) Autentizace v elektronických kanálech

77. Podle ustanovení § 23 odst. 5 písm. c) vyhlášky č. 163/2014 Sb. povinná osoba zabezpečuje ochranu informačních a komunikačních systémů před přístupem a zásahy ze strany neoprávněných osob a před poškozením a možnost zpětně získat stanovené informace i v případě, že k poškození došlo.

78. Podle bodu 31 písm. g) Obecných pokynů EBA/GL/2019/04 by finanční instituce měly prosazovat metody ověření, které jsou dostatečně robustní, aby přiměřeně a účinně zajistily dodržování zásad a postupů kontroly přístupu. Metody ověření by měly odpovídat

[81] Dle zápisu z 1. jednání Výboru pro bezpečnost ze dne 13.5.2021 v souboru „*Zápis z jednání 20210513.docx*“ byl zaznamenán znatelný nárůst phishingu na klientech i zaměstnancích (45 případů v prvním čtvrtletí 2021).
[82] Počátek kontrolního období.
[83] Poslední den před provedením outsourcingu do RBCZ.

kritičnosti systémů IKT, informací nebo procesu, k nimž se přistupuje. Měly by zahrnovat přinejmenším složitá hesla nebo silnější metody ověření (například dvoufaktorové ověření) podle příslušného rizika.

79. Pro klientskou správu smluv a úvěrových účtů účastník řízení v době Kontroly webový kanál CIBIS Web pod obchodním názvem Internet Servis. Klientská autentizace do aplikace probíhala na webové stránce sis.rsts.cz zadáním uživatelského jména a hesla. Po ověření měl klient přístup ke svým osobním údajům včetně zůstatků na účtech. U vybraných aktivních operací (jako např. změna údajů nebo změna smlouvy o stavebním spoření) bylo navíc požadováno zadání jednorázového kódu poslaného v SMS na zaregistrovaný telefon klienta.

80. V souvislosti s autentizací heslem bylo zjištěno, že složitost klientského hesla musela být minimálně na úrovni „*střední*“, což dle vyjádření účastníka řízení znamená, že „*heslo musí mít minimálně 8 znaků a zároveň obsahovat velké, malé písmeno a číslo.*“[84] Při této konfiguraci je uživatelem systému možné zvolit oblíbená a útočníkem odhadnutelná hesla. Při obnově zapomenutého hesla nebo nastavení nového hesla např. při jeho kompromitaci lze využít webový formulář, kde je uvedeno: „*Po vyplnění žádosti o obnovení přístupu bude vygenerováno jednorázové heslo, které Vám zašleme do několika minut na registrovaný mobilní telefon.*“ [85] V žádosti o obnovení je potřeba vyplnit pouze uživatelské jméno, datum narození, 1. a 3. znak rodného čísla za lomítkem a opsat kód z obrázku. Při přístupu k telefonu klienta nebo instalovaném malware na tomto telefonu může dojít při znalosti osobních údajů klienta ke kompromitaci a zneužití hesla. Účastník řízení navíc zaznamenal nárůst pokusů o phishing na své klienty i zaměstnance[86], z čehož vyplývá poptávka po zneužití elektronických kanálů účastníka řízení. Zneužití hesla úspěšným phishingovým útokem správní orgán považuje mezi výše uvedenými scénáři za nejsnáze proveditelné a nejpravděpodobnější narušení bezpečnosti elektronických kanálů.

81. Vzhledem k výše uvedeným slabinám správní orgán považuje **autentizaci pouze heslem do klientské webové aplikace účastníka řízení za nedostatečnou.** Druhý faktor u některých aktivních operací zmírňuje rizika neautorizovaných změn, nicméně nemá vliv na riziko neautorizovaného přístupu k osobním i citlivým datům klienta a ztráty reputace účastníka řízení.

82. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 30.6.2020[87] do 31.5.2021[88] nepoužíval dostatečně robustní metody autorizace pro vstup do klientské webové aplikace, k němuž vyžadoval pouze heslo o složitosti ve stupni „střední“, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 23 odst. 5 písm. c) vyhlášky č. 163/2014 Sb. ve spojení s bodem 31 písm. g) Obecných pokynů EBA/GL/2019/04.**

[84] Viz soubor „*Doplnění elektronických kanálů.docx*“ předložený dne 2.11.2021, spis, č. l. 5 (DVD).
[85] V době Kontroly dostupný z: https://sis.rsts.cz/cibis-web/mvc/security/zadost-o-obnoveni-pristupu
[86] Dle zápisu z 1. jednání Výboru pro bezpečnost ze dne 13.5.2021 byl zaznamenán znatelný nárůst phishingu na klientech i zaměstnancích (45 případů v prvním čtvrtletí 2021). Viz soubor „*Zápis z jednání 20210513.docx*“, spis, č. l. 5 (DVD). Dále byla doložena e-mailová korespondence k šesti příkladům phishingu z let 2020 a 2021 (Viz soubory ve složce „*phishing po klientech*“ předané dne 2.11.2021, spis, č. l. 5 (DVD)).
[87] Datum účinnosti Obecných pokynů EBA/GL/2019/04
[88] Poslední den před provedením outsourcingu do RBCZ.

b) Prověřování bezpečnosti elektronických kanálů

83. Podle ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. povinná osoba zabezpečí, že proces rozpoznávání rizik je zajištěn u všech činností a na všech řídicích a organizačních úrovních a umožňuje odhalování nových, dosud neidentifikovaných rizik.

84. Podle bodu 21 písm. e) přílohy č. 6 k vyhlášce č. 163/2014 Sb. při provozování informačních systémů povinná osoba zejména zajistí pravidelné prověřování a vyhodnocování bezpečnosti informačních systémů.

85. Dle kap. 9.1.1 skupinové politiky RBI Application Security Standard[89] musí být všechny kritické aplikace, mezi něž jsou zařazeny i aplikace s klientským přístupem a přímé kanály, minimálně jednou ročně předmětem penetračního testování. Testy provedené společností AEC v červenci 2021[90] nebyly primárně zaměřeny na zranitelnosti webové aplikace.[91] Dále k aplikaci CIBIS Web nebyly zpracovány analýzy rizik, ve kterých by byla vyhodnocena rizika související s provozem a bezpečností tohoto přímého kanálu a případně navržena zmírňující opatření. Z uvedeného vyplývá, že účastník řízení **nedostatečně řídil IT rizika spojená s webovou aplikací CIBIS Web** a neměl tak dostatečné ujištění o úrovni bezpečnosti tohoto systému.

86. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 1.1.2019[92] do 22.7.2021[93] neprováděl penetrační testy aplikace CIBIS Web, který je přímo dostupný ze sítě internet a při jeho ovládnutí lze přistupovat ke klientským datům, a neměl tak informace o úrovni bezpečnosti tohoto systému, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb. a v bodě 21 písm. e) přílohy č. 6 k vyhlášce č. 163/2014 Sb.**

vi) <u>Pohotovostní plánování</u>

87. Podle bodu 10 přílohy č. 6 k vyhlášce č. 163/2014 Sb. povinná osoba zavede a udržuje pohotovostní plány pro případy neplánovaného porušení nebo omezení svých činností, selhání pro povinnou osobu významných třetích osob nebo selhání vnější infrastruktury.

88. Podle bodu 11 písm. d) a e) přílohy č. 6 k vyhlášce č. 163/2014 Sb. povinná osoba v pohotovostních plánech stanoví alespoň způsob zajištění nouzového provozu s uvedením minimálních funkcí, které zůstanou zachovány, a způsob obnovy činností včetně činností zajišťovaných třetími osobami.

89. Podle odst. 78 Obecných pokynů EBA/GL/2019/04 by finanční instituce v rámci řádného řízení kontinuity činnosti měly provádět analýzu dopadu na podnikatelskou činnost analyzováním své expozice vůči závažným narušením činnosti a posouzením jejich možných dopadů (včetně dopadů v oblasti důvěrnosti, integrity a dostupnosti), a to kvantitativně i kvalitativně, pomocí interních nebo externích údajů (např. údajů externích poskytovatelů významných pro obchodní proces nebo veřejně dostupných údajů, které

[89] Viz soubor „*SUP-2018-0149_RBI Group Application Security Standard_V1.4.pdf*“ spis, č. l. 5 (DVD).
[90] Viz soubor „*AEC_PT_RBCZ_Infrastruktura_RSTS_report_v2.pdf*“, spis, č. l. 5 (DVD).
[91] Kapitola 2.1. Zprávy z penetračních testů infrastruktury účastníka řízení: „*Předmětem projektu byly penetrační testy externí a interní infrastruktury Raiffeisen stavební spořitelna a.s. a průzkum internetu za účelem nalezení uniklých hesel zaměstnanců*.“
[92] Počátek kontrolního období.
[93] Datum vypracování výsledné zprávy penetračních testů infrastruktury účastníka řízení.

mohou být z hlediska analýzy dopadu na podnikatelskou činnost relevantní), a analýzu scénářů. Analýza dopadu na podnikatelskou činnost by také měla zvážit kritičnost identifikovaných a klasifikovaných obchodních funkcí, podpůrných procesů, třetích stran a informačních aktiv a jejich vzájemné závislosti.

90. Podle odst. 80 Obecných pokynů EBA/GL/2019/04 by finanční instituce na základě svých analýz dopadu na podnikatelskou činnost měly vypracovat plány k zajištění kontinuity činnosti (plány kontinuity činnosti), které by měly být zdokumentovány a měl by je schválit vedoucí orgán finanční instituce. Plány by měly brát v úvahu zvláště rizika, která by mohla mít nepříznivý dopad na systémy IKT a služby v oblasti IKT. Plány by měly podporovat cíle týkající se ochrany a v případě potřeby obnovy důvěrnosti, integrity a dostupnosti obchodních funkcí finančních institucí, podpůrných procesů a informačních aktiv. Finanční instituce by měly při sestavování těchto plánů podle potřeby koordinovat svou činnost s příslušnými interními a externími zainteresovanými stranami.

91. Podle odst. 82 Obecných pokynů EBA/GL/2019/04 by finanční instituce měla ve svém plánu kontinuity činnosti zvážit řadu různých scénářů, včetně extrémních, ale věrohodných scénářů, kterým může být vystavena, a to včetně scénáře kybernetického útoku, a měla by posoudit možný dopad takových scénářů. Na základě těchto scénářů by finanční instituce měla popsat, jak je zajištěna kontinuita systémů IKT a služeb v oblasti IKT, jakož i bezpečnost informací finanční instituce.

92. Podle odst. 89 písm. a) a c) Obecných pokynů EBA/GL/2019/04 by plány kontinuity činnosti finanční instituce měly zahrnovat a) testování vhodného souboru závažných, ale pravděpodobných scénářů, včetně scénářů zvažovaných pro vývoj plánů kontinuity činnosti (a případně testování služeb poskytovaných třetími stranami); měl by sem spadat převod důležitých obchodních funkcí, podpůrných procesů a informačních aktiv do prostředí pro obnovu po havárii a prokázání toho, že je lze takto provozovat po dostatečně reprezentativní časové období a že poté lze obnovit obvyklou činnost; a c) postupy k ověření schopnosti zaměstnanců a dodavatelů, systémů IKT a služeb v oblasti IKT provozovaných finančními institucemi přiměřeně reagovat na scénáře vymezené v bodě 89 písm. a).

93. Účastník řízení vypracoval a předložil sadu pohotovostních plánů kontinuity obchodní činnosti (z angl. *business continuity*, dále jen „BC“).[94]. Přezkoumáním obsahu předložených BC plánů správní orgán zjistil, že v nich účastník řízení dostatečně nestanovil způsob obnovy svých činností a způsob zajištění nouzového provozu s uvedením minimálních funkcí, které zůstanou zachovány, a způsob obnovy těchto činností. Předložené BC plány byly omezené pouze na seznam participujících pracovníků a obsahovaly pouze prioritizaci činností.

94. Účastník řízení v rámci Kontroly doložil pouze jeden BC test, a to navíc pouze pro jeden scénář – „*Dostupnost IS CIBIS ze záložního centra Nagano*“ – provedený naposledy dne 27.7.2018.[95] Žádné jiné BC testy účastník řízení v rámci kontrolního období neprovedl. Účastník řízení dále nezpracoval očekávané scénáře BC do BC plánů, např. „*Selhání lidských zdrojů*“ nebo „*Selhání IS/IT*“ – jediný provedený BC test byl omezený pouze na

[94] Jednotlivé pohotovostní BC plány pro oblasti obchodní činnosti účastníka řízení. Viz jednotlivé soubory s názvy BCP*.xlsx ve složce „*D4 BCM_securita_predpisy*“, spis, č. l. 5 (DVD).
[95] Záznam o provedení testu ze dne 27.7.2018. Viz soubor „*20180727_Test provozu IS CIBIS_Nagano_sken.pdf*“, spis, č. l. 5 (DVD).

obnovu služeb IS/IT, nikoliv na činnosti v celém obchodním procesu.

95. **Existence prověřených postupů obnovy včetně způsobu zajištění prostředků nutných pro nouzový provoz činností útvarů je klíčovým nástrojem pro minimalizaci škody a doby obnovy po BCM události.** Účastník řízení se výše uvedenými nedostatky vystavuje riziku delší doby trvání procesu obnovy, riziku finančních dopadů a s tím souvisejícímu reputačnímu riziku.

96. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 30.6.2020[96] do 31.5.2021[97] nezavedl pohotovostní plánování pro všechny důležité obchodní a pomocné procesy a pro scénáře nad rámec výpadků IS/IT, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení bodu 10 a bodu 11 písm. d) a e) přílohy č. 6 k vyhlášce č. 163/2014 Sb. ve spojení s body 78, 80, 82 a 89 písm. a) a c) Obecných pokynů EBA/GL/2019/04.**

vii) <u>Vnitřní audit v oblasti IS/IT</u>

97. Podle bodu 17 přílohy č. 8 k vyhlášce č. 163/2014 Sb. vede povinná osoba pro každou jednotlivou auditní akci auditorský spis. Auditorský spis je veden takovým způsobem, aby byl plně rekonstruovatelný postup při provedeném auditu. Auditorské spisy jsou prověřovány osobou ve vedení funkce vnitřního auditu nebo jí zmocněným vnitřním auditorem.

98. Podle plánu vnitřního auditu účastníka řízení[98] probíhal každé dva roky audit „*Operation and Security*“, který pokrýval IS/IT oblast. Dále každý rok pak probíhal audit „*Operational Risk Management*“, který zahrnoval oblast outsourcingu. V rámci kontroly na místě si správní orgán vyžádal auditní spisy k auditům 2/2020 *Operation and Security*[99] a 6/2020 *Operational Risk Management*.[100]

99. Dne 7.12.2021 proběhla schůzka správního orgánu s auditorem odpovědným za výše zmíněné audity. V rámci auditu 2/2020 *Operation and Security* vznikl dokument „*Checklist - provoz a bezpečnost*“[101], který obsahuje plán auditu a negativní zjištění. **Z dodaných podkladů však nelze dostatečně rekonstruovat činnost auditora a nelze tak posoudit, že audit dostatečně prověřil celou IS/IT oblast.** V rámci auditu 6/2020 *Operational Risk Management* nebyl kontrolnímu týmu doložen žádný podklad, který by rekonstruoval činnost auditora.

100. **Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení v období od 24.2.2020[102] do 20.5.2020[103] v případě auditu 2/2020 *Operation and***

[96] Datum účinnosti Obecných pokynů EBA/GL/2019/04
[97] Poslední den před provedením outsourcingu do RBCZ.
[98] Plány vnitřního auditu účastníka řízení za roky 2019 - 2021. Viz soubory „*03_Annual audit plan 2019_allocation.xlsx*“, „*03_Annual audit plan 2020_allocation II.xlsx*“ a „*03_Annual audit plan 2021_allocation.xlsx*“, vše spis, č. l. 5 (DVD).
[99] Auditní spis k auditu 2/2020 *Operation and Security*. Viz jednotlivé soubory ve složce „*3_Provoz a bezpecnost_auditni_spis*“, spis, č. l. 5 (DVD).
[100] Auditní spis k auditu 6/2020 *Operational Risk Management*. Viz jednotlivé soubory ve složce „*5_Audit outsourcingu*“, spis, č. l. 5 (DVD).
[101] Viz soubor „*Checklist_provoz a bezpecnost.docx*“, spis, č. l. 5 (DVD).
[102] Počátek auditu *Operation and Security*.
[103] Vyhotovení auditní zprávy v rámci auditu *Operation and Security*.

***Security* a v období od 25.5.2020[104] do 26.8.2020[105] v případě auditu 6/2020 *Operational Risk Management* nevedl auditorský spis způsobem, který by umožňoval plnou rekonstruovatelnost, čímž postupoval v rozporu s požadavkem upřesněným v ustanovení bodu 17 přílohy č. 8 k vyhlášce č. 163/2014 Sb.**

D. Shrnutí

101. V souladu s ustanovením § 8b odst. 2 zákona o bankách správní orgán uzavírá, že řídicí a kontrolní systém účastníka řízení musí být účinný, ucelený a přiměřený povaze, rozsahu a složitosti rizik spojených s modelem podnikání a činností, a to v jeho celku i částech po celou dobu existence účastníka řízení jakožto licencované banky. Jak je shora v jednotlivých bodech popsáno, vykazoval řídicí a kontrolní systém účastníka řízení nedostatky v řadě podoblastí řízení rizik informačních systémů a informačních technologií v souhrnném období od 1.1.2019 do 15.10.2021, kdy den 1.1.2019 je počátkem kontrolovaného období, den 15.10.2021 pak nejzazším datem, ke kterému trval poslední z postihovaných nedostatků v rámci řídicího a kontrolního systému.

E. Sankce

102. Ustanovení § 36j ZoB stanoví, že přestupky podle tohoto zákona projednává Česká národní banka.

103. Přestupkový zákon umožňuje uložení alternativních druhů trestů (např. napomenutí)[106] a popř. modifikaci trestu (např. podmíněné upuštění od uložení správního trestu).[107] S ohledem na závažnost protiprávního jednání účastníka řízení v tomto konkrétním případě však nepřipadá aplikace alternativních druhů trestání ani modifikace trestu v úvahu. Jako nejefektivnější prostředek, který zajistí naplnění individuálně a generálně preventivního i represivního účelu sankce, se jeví uložení pokuty.

104. Podle ustanovení § 36e odst. 6 písm. f) zákona o bankách lze za přestupek podle odstavce 2 písm. a) téhož zákonného ustanovení uložit pokutu do výše dvojnásobku výše neoprávněného prospěchu, jde-li o přestupek podle odstavce 2 nebo odstavce 3 písm. c) a spáchala-li ho ovládaná banka; není-li možné výši neoprávněného prospěchu zjistit, lze uložit pokutu do výše 10 % čistého ročního obratu vyplývajícího z konsolidované účetní závěrky ovládající osoby za bezprostředně předcházející účetní období.

105. Vzhledem k tomu, že otázka neoprávněného prospěchu nebyla předmětem tohoto řízení, přistoupil správní orgán k uložení pokuty dle výše čistého obratu ovládající osoby. Čistý obrat ovládající osoby RBCZ v předchozích letech dosahoval výše 10 mld. Kč[108], horní hranice pokuty tak činí částku 1 mld. Kč. Správní orgán konstatuje, že uložením pokuty ve výši 100 000 Kč nebyla překročena horní hranice možné pokuty.

106. K možné liberaci účastníka řízení podle § 21 odst. 1 a 2 přestupkového zákona správní orgán uvádí, že mu není známo, že by účastník řízení vynaložil veškeré úsilí, které po něm bylo možné požadovat, aby přestupku uvedenému v tomto příkaze zabránil.

---

[104] Počátek auditu *Operational Risk Management*.
[105] Vyhotovení auditní zprávy v rámci auditu *Operational Risk Management*.
[106] Viz ustanovení § 35, § 45, § 47 až § 50 přestupkového zákona.
[107] Viz ustanovení § 42 až § 44 přestupkového zákona.
[108] Údaje o čistém obratu z konsolidovaných účetních závěrek RBCZ. Dostupné z: https://www.rb.cz/o-nas/kdo-jsme/vysledky-hospodareni/vyrocni-zpravy.

107. Správní orgán se při určování **druhu správního trestu** a **jeho výměry** řídil zásadami uvedenými v ustanovení § 37 přestupkového zákona, povahu a závažnost přestupku posoudil dle ustanovení § 38 přestupkového zákona, a zároveň neshledal ve vytýkaném pochybení žádné významné polehčující či přitěžující okolnosti ve smyslu ustanovení § 39 a § 40 přestupkového zákona. Správní orgán taktéž přihlédl k povaze činnosti právnické osoby a obecným právním zásadám, zejména k zásadě individualizace sankce a k zásadě legitimního očekávání.

108. Účastník řízení je **profesionálním subjektem** působícím v oblasti poskytování bankovních služeb desítky let, a proto není možné přejít jeho pochybení, kterým naplnil skutkovou podstatu přestupku podle ustanovení § 36e odst. 2 písm. a) zákona o bankách. Účastník řízení právě jako profesionální subjekt znal, či měl a mohl znát povinnosti stanovené v zákoně o bankách a ve vyhlášce č. 163/2014 Sb.

109. Podle ustanovení § 38 přestupkového zákona je **povaha a závažnost** přestupku dána zejména: významem zákonem chráněného zájmu, který byl přestupkem porušen nebo ohrožen, významem a rozsahem následku přestupku, způsobem spáchání přestupku, okolnostmi spáchání přestupku a délkou doby, po kterou trvalo protiprávní jednání pachatele nebo po kterou trval protiprávní stav udržovaný protiprávním jednáním pachatele. Rovněž v tomto případě se jedná o demonstrativní výčet.

110. Pokud jde o **povahu** projednávaného přestupku, jde o **přestupek trvající**, kdy účastník řízení vyvolal protiprávní stav tím, že nedisponoval řídícím a kontrolním systémem, který je nepřetržitě a v celém svém rozsahu funkční a který splňuje všechny požadavky stanovené ZoB a právním předpisem jej provádějícím.

111. K povaze a závažnosti přestupku správní orgán dále uvádí, že jeho **objektem**, tedy zákonem chráněným zájmem, za který správní orgán ukládá sankci, je **řádný a obezřetný výkon činnosti stavební spořitelny, který je možný pouze při současné existenci a uplatňování funkčního a efektivního řídicího a kontrolního systému.**

112. Co se týče **významu a rozsahu následku přestupku**, lze uvést, že společenskou škodlivost reflektuje ustanovení § 36 odst. 6 písm. f) zákona o bankách, když umožňuje za přestupek uložit pokutu až do výše dvojnásobku výše neoprávněného prospěchu; není-li možné výši neoprávněného prospěchu zjistit, lze uložit pokutu do výše 10 % čistého ročního obratu dosaženého bankou za bezprostředně předcházející účetní období. Individuální společenská škodlivost přestupku pak spočívá zejména ve skutečnosti, že nefunkční řídicí a kontrolní systém v oblasti řízení rizik informačních systémů a informačních technologií mohl mít vážné důsledky s dopadem na majetek účastníka řízení.

113. Pokud se týká **způsobu spáchání přestupku**, jedná se o přestupek **omisivní** povahy, tedy nesplnění povinnosti uložené právními předpisy, neboť účastník byl povinen disponovat řídícím a kontrolní systémem, který splňuje všechny požadavky stanovené ZoB a vyhláškou č. 163/2014 Sb.

114. Co se týče otázky **zavinění**, jedná se o přestupek založený na principu objektivní odpovědnosti, tedy odpovědnosti za výsledek, kdy se **konkrétní zavinění nezkoumá.**

115. Pokud jde o **účinek** protiprávního jednání účastníka řízení, k naplnění skutkové podstaty přestupku dochází bez ohledu na skutečnost, zda v konkrétním případě dojde příslušným jednáním ke vzniku škody na majetku zákazníků či nikoli. Vznik škody netvoří obligatorní znak skutkové podstaty tohoto přestupku. Správní orgán proto vznik škody podrobněji nezkoumal a nekvantifikoval.

116. Správní orgán se také zabýval **majetkovými poměry** účastníka řízení. Správní orgán vycházel při hodnocení majetkových poměrů z posledních známých finančních ukazatelů, a to za rok 2021.[109] Účastník řízení vykázal čistý zisk 443 mil. Kč a jeho vlastní kapitál k 31.12.2021 dosáhl 5 422 mil. Kč.

117. Na základě posouzení všech uvedených skutečností dospěl správní orgán k jednoznačnému závěru, že pokuta uložená při dolní hranici zákonné sazby odpovídá závažnosti protiprávního jednání účastníka řízení a okolnostem, za nichž se jej dopustil. Uložená pokuta zároveň zásadním způsobem nedopadá do majetkových poměrů účastníka řízení a koresponduje s ustálenou rozhodovací praxí správního orgánu v obdobných případech.

118. Ustanovení § 90 odst. 1 přestupkového zákona ve spojení s ustanovením § 150 odst. 1 správního řádu umožňuje správnímu orgánu v řízení z moci úřední uložit povinnost formou písemného příkazu, a to jako první úkon v řízení. Správní orgán přistoupil k vydání příkazu, neboť v tomto případě považuje skutková zjištění za dostatečná.

P O U Č E N Í

Proti tomuto příkazu lze podat odpor podle ustanovení § 150 odst. 3 správního řádu u sekce licenčních a sankčních řízení České národní banky, se sídlem Na Příkopě 28, 115 03 Praha 1, a to **do 8 dnů** ode dne doručení tohoto příkazu. Podáním odporu se příkaz ruší a v řízení se pokračuje. Zpětvzetí odporu není přípustné. Příkaz, proti němuž nebyl podán odpor, se stává pravomocným a vykonatelným rozhodnutím.

Pro případ podání odporu správní orgán poučuje účastníka řízení v souladu s ustanovením § 80 odst. 2 přestupkového zákona o jeho právu požádat o nařízení ústního jednání. Správní orgán není návrhem účastníka řízení ve věci nařízení ústního jednání vázán a ústní jednání nařídí, je-li to nezbytné pro zjištění stavu věci, nebo pro uplatnění práv účastníka řízení.

Ing. Karel Gabrhel LL.M.
ředitel sekce licenčních a sankčních řízení
podepsáno elektronicky

Mgr. et Mgr. Petra Chroustovská
ředitelka odboru sankčních řízení
podepsáno elektronicky

[109] Účetní závěrka účastníka řízení za rok 2021, dostupné z:
h https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=72181556&subjektId=449350&spis=74797.