ČESKÁ REPUBLIKA

ROZSUDEK
JMÉNEM REPUBLIKY

Městský soud v Praze rozhodl v senátě složeném z předsedy JUDr. Slavomíra Nováka a soudkyň Mgr. Jany Jurečkové a Mgr. Andrey Veselé ve věci

žalobkyně: **Iuridicum Remedium, z. s.**, IČO: 26534487
sídlem Přístavní 1236/35, 170 00 Praha 7
zastoupená advokátem Mgr. et Mgr. Janem Vobořilem
sídlem U Smaltovny 32/1115, 170 00 Praha 7

proti

žalovanému: **Ministerstvo vnitra**
sídlem Nad Štolou 3, 170 43 Praha 7

o žalobě proti rozhodnutí ministra vnitra ze dne 16. 3. 2023, sp. zn. MV-35377-3/SO-2023,

takto:

I. Žaloba se zamítá.

II. Žádný z účastníků nemá právo na náhradu nákladů řízení.

Shodu s prvopisem potvrzuje J. V.

Odůvodnění:

I.
Základ sporu

1. Žalobkyně se domáhá zrušení rozhodnutí ministra vnitra ze dne 16. 3. 2023, č. j. MV-35377-3/SO2023 (dále jen „*napadené rozhodnutí*"), jímž byl zamítnut její rozklad proti rozhodnutí Ministerstva vnitra, odboru eGovernmentu (dále jen „*správní orgán I. stupně*") ze dne 17. 1. 2023, č. j. MV-842-1/EG-2023 (dále jen „*prvostupňové rozhodnutí*"), kterým byla částečně odmítnuta žádost žalobkyně o poskytnutí informace v bodě 9. a zcela odmítnuta v bodech 3., 4. a 8., a to podle § 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „*InfZ*"), ve spojení s § 10a 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*").

2. V bodech 3., 4., 8. a 9. žádosti požádala žalobkyně o následující dokumentaci:

   3. Kompletní dokumentaci Enterprise Architecture, včetně všech relevantních příloh. Nejlépe ve zdrojovém datovém formátu a export do formátu PDF. Tato dokumentace je pro tento typ projektů vyžadována Odborem Hlavního Architekta eGovernmentu MVČR,

   4. Kompletní dokumentaci bezpečnostní architektury, dokumentaci bezpečnostní politiky dle § 5 odst. 2 písm. c) zákona o kybernetické bezpečnosti a dále dokumentaci bezpečnostních požadavků na dodavatele dle § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti,

   8. Seznam software a hardware, který je využit v architektuře ISDS, včetně vybavení s oprávnění přístupu do ISDS (počítače administrátorů atd.), a vyžadoval online aktivaci, a nebo má povolenu online aktualizaci,

   9. Seznam všech externích auditů provedených na ISDS a obslužném vybavení (pokud byly provedeny) včetně auditů provedených u zpracovatelů podílejících se na provozu systému ISDS, s definicí rozsahu auditu, jeho závěry a doložením kvalifikace auditora k dané odbornosti.

II.
Obsah žaloby a vyjádření žalovaného

3. **V prvním žalobním bodu** žalobkyně namítala nepřezkoumatelnost napadeného rozhodnutí. Uvedla, že argumentaci správních orgánů lze shrnout do teze, že jakékoli dokumenty týkající se IT řešení informačního systému datových schránek mají být utajovány, protože jejich vyzrazení může ohrozit bezpečnost. S takovým přístupem, který rezignuje na jasné označení rizik včetně řešení otázky jejich významu a toho, zda jde o přímou hrozbu, by ovšem došlo k absolutnímu vyprázdnění práva na svobodný přístup k informacím o jakýchkoli IT systémech veřejné správy, protože bezpečnost teoreticky může ohrozit poskytnutí jakékoli informace. Zabezpečení obdobných systémů se přitom zásadně nemůže opírat o skutečnost, jestli nějaké informace budou veřejné nebo nikoli, proto ani jejich uveřejnění nemůže mít dopad na významné či přímé snížení bezpečnosti takového

systému. Je nezbytné rozlišovat, zda žadatel žádá o přihlašovací údaje správce IS nebo o základní „big picture“ model architektury a bezpečnostní politiky, které nemají obsahovat žádné implementační detaily. Tento přístup je v přímém rozporu s metodikami zabezpečení IT systémů, které v rámci principu Secure from design uplatňují základní pravidlo, že bezpečnost systému nemá záviset na utajení implementace nebo jejích součástí.

4. Žalovaný se dále nevypořádal s argumentací žalobkyně zpochybňující závěry správního orgánu I. stupně k jednotlivým bodům žádosti a vůbec nereagoval na námitku, že správní orgán I. stupně nepracuje s možností neposkytnutí pouze části požadované informace – zejména u odpovědí na otázky č. 3, 4, 8 a 9. Správní orgány se tedy nevěnovaly podrobně jednotlivým částem požadovaných informací a nehodnotily možnost jejich částečného poskytnutí.

5. Ve druhém žalobním bodu žalobkyně namítala, že jako důvod odmítnutí je uveden § 11 odst. 1 písm. d) InfZ. Správní orgány však jednoznačně neuvádí, v čem konkrétně spatřují významné nebo přímé ohrožení. Je evidentní, že minimálně část z požadovaných a odmítnutých informací nemůže nijak přispět k provedení případného kybernetického útoku.

6. Například v bodě 4 byly požadovány informace o bezpečnostní politice a o bezpečnostních požadavcích na subdodavatele v souvislosti s informačním systémem datových schránek, přičemž žalobkyni není jasné, v čem je ohrožující sdělit veřejnosti obecné informace o bezpečnostním nastavení systému, které obvykle kopírují příslušné použité technické normy, které jsou běžně dostupné, či v čem je ohrožující sdělit, jaká bezpečnostní kritéria byla volena při výběru subdodavatelů. Nepochybně celá řada informací, které se týkají bezpečnostních politik, je u obdobných systémů zcela očekávatelná a informace, že systém funguje právě tímto způsobem, není nijak překvapující ani ohrožující.

7. Pokud jde o informace o použitém hardwaru a softwaru (dotaz č. 8), žalobkyně se dotazovala pouze na software a hardware, které vyžadují online aktivaci, anebo mají povolenou online aktualizaci. Nepožadovala tedy informaci o tom, zda jsou dostupné online pro útočníka, což by skutečně mohlo ohrozit jeho bezpečnost. Pokud by existovalo reálné ohrožení u konkrétních používaných produktů, pak nepochybně nikoli u všech, a měla být opět poskytnuta minimálně částečná informace s odůvodněním odmítnutí vázaného na konkrétní software a hardware s popisem konkrétních rizik.

8. V části vázané k dotazu č. 9 pak bylo odmítnuto sdělení výsledků auditů. Opět jde o zcela zásadní informaci pro hodnocení toho, jakým způsobem je nakládáno s vysoce citlivými informacemi v systému datových schránek. Pokud audity doporučily některé změny, pak tyto již měly být přijaty, a tedy sdělení závěrů auditu nepředstavují žádné ohrožení bezpečnosti ISDS. Pokud žádné závady zjištěny nebyly, není důvod toto jako informaci nesdělit. I zde tak měly správní orgány zvažovat minimálně poskytnutí částí těchto závěrů. Pouhá informace, že byly zjištěny nedostatky, je pro někoho, kdo se rozhoduje o tom, zda si zřídí datovou schránku, důležitá, i pokud nebude znát detaily těchto vad, a informace o zjištění blíže neupřesněných vad v minulosti je zcela nezneužitelná k jakémukoli kybernetickému útoku.

9. Žalovaný ve svém vyjádření navrhl žalobu jako nedůvodnou zamítnout.

10. K námitce nepřezkoumatelnosti napadeného rozhodnutí uvedl, že se v něm ztotožnil s argumentací správního orgánu I. stupně, pokud jde o důvody odmítnutí, přičemž z

odůvodnění prvostupňového rozhodnutí je zřejmé, proč rozhodl právě tak, jak rozhodl. S jeho argumentací ostatně žalobkyně v řízení částečně polemizuje, což by při nepřezkoumatelnosti rozhodnutí nebylo možné.

11. K dalším námitkám žalovaný odkázal na pojem z oblasti počítačové bezpečnosti, Security through obscurity (bezpečnost skrze neznalost), což je označení používané v počítačové bezpečnosti. Bezpečnost skrze utajení používá utajení (například návrhu, implementace atd.) tím, že používá nestandardní konstrukce či postupy (např. vlastní algoritmy pro šifrování nebo hashování, vlastní úpravy všeobecně uznávaných algoritmů nebo ukládání přístupových údajů tak, že jsou veřejně přístupné, pouze jsou nějak zamaskované apod.) k zajištění bezpečnosti. Systém využívající tohoto principu však může obsahovat programátorské chyby i bezpečnostní rizika, ale jeho tvůrce věří, že pokud tyto bezpečnostní chyby nejsou známé a např. přístupové údaje jsou jen těžko zjistitelné, je nepravděpodobné, že by na ně útočník přišel. Bezpečnost skrze utajení je důvěra v to, že jakýkoliv systém může být bezpečný po dobu, kdy nikomu, kromě lidí, kteří ho implementovali, není dovoleno zjistit nic o jeho vnitřních mechanismech. Například schovávání hesla do binárního souboru či skriptu s tím, že subjekt předpokládá, že ho nikdy nikdo nenajde, je základní případ bezpečnosti skrze utajení. Tento přístup je upřednostňován většinou byrokratických organizací (vlády, armádní složky a průmyslové podniky) a býval využíván jako hlavní prostředek „pseudobezpečnosti“ v počítačových systémech.

12. § 11 odst. 1 písm. d) InfZ byl zákonodárcem přijat za účelem vytvoření výluk z práva na informace, což podporuje též důvodová zpráva. Pojem bezpečnostní opatření je pojmem, který dopadá na širokou paletu konkrétních případů, a je nutné je v daném kontextu vykládat tak, aby poskytnutím informace nedošlo k nenapravitelnému ohrožení účinnosti bezpečnostního opatření. Informace, nemá-li být poskytnuta, musí významně nebo přímo ohrožovat účinnost bezpečnostního opatření na základě zvláštního předpisu pro účely ochrany bezpečnosti osob, majetku a veřejného pořádku. V daném případě je tímto zvláštním předpisem zákon o kybernetické bezpečnosti a další předpisy v oblasti kybernetické bezpečnosti, například vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „*Vyhláška č. 82/2018 Sb.*“). Právní předpisy v oblasti kybernetické bezpečnosti jsou přijaty právě za účelem ochrany bezpečnosti osob, majetku a veřejného pořádku.

13. V daném případě je potenciální poskytnutí dokumentace bezpečnostní architektury informačního systému datových schránek, případně provedených auditů, takovou informací, která může ohrozit funkčnost informačního systému datových schránek (dále též jen „*ISDS*“). Toto nebezpečí lze vyhodnotit jako významné nebo přímo ohrožující. Jako konkrétní příklad ohrožení lze uvést informace z auditů popisující nedostatky daného systému, kdy na základě této informace by žadatel mohl získat přehled o obecně zranitelných místech tohoto prvku kritické informační infrastruktury, což je z pohledu zajištění bezpečnosti nanejvýš rizikové. K neposkytnutí požadovaných informací tedy nedochází na základě arbitrárního rozhodnutí, ale v souladu se schválenou a přijatou politikou povinného subjektu, na základě zákona a s cílem ochránit zákonem chráněné zájmy. Vzhledem k tomu, že ISDS je systémem kritické informační infrastruktury a právními předpisy je požadována maximální míra jeho zabezpečení, riziko ohrožení účinnosti bezpečnostních opatření je v případě poskytnutí požadovaných informací významné a přímé.

14. Odmítnutí poskytnutí požadovaných informací bylo v napadeném rozhodnutí odůvodněno ve spojení s § 10a zákona o kybernetické bezpečnosti, které je ve vztahu k InfZ speciálním důvodem pro neposkytnutí informací a do zákona o kybernetické bezpečnosti bylo zařazeno s ohledem na rostoucí počet informačních systémů, včetně systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy jinak povinné subjekty podle InfZ, a rovněž se zohledněním rostoucího počtu útoků v kybernetickém prostoru. Ustanovení § 10a zákona o kybernetické bezpečnosti proto ve vztahu k předmětné žádosti umožňuje neposkytovat dle InfZ takové informace, jejich zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti a účinnost opatření vydaného podle zákona o kybernetické bezpečnosti. V obou uvedených případech platí pouhá možnost ohrožení kybernetické bezpečnosti, tj. k samotnému přímému ohrožení nemusí dojít, ale pro neposkytnutí informací podle InfZ postačuje pouhá pravděpodobnost ohrožení.

15. Dílčí či některé informace, jako aktiva, jsou označeny z hlediska důvěrnosti stupněm „vysoká“ podle Vyhlášky č. 82/2018 Sb., přičemž tyto informace tvoří uzavřený kruh, kdy při zveřejnění jedné jeho složky může být ohrožena bezpečnost a tím i důvěra v celý zbytek informačního systému. Bezpečnostní audit ISDS (zpráva jako celek) je pak označen jako „citlivé – interní“. Bezpečnostní audit ISDS obsahuje technické specifikace a konfigurační parametry, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti. Jejich poskytnutím by byly zpřístupněny informace, které mohou být zneužity při potencionálním kybernetickém útoku, k zacílení kybernetického útoku a způsobení závažnějších následků kybernetického útoku. Riziko kybernetického útoku by se tedy razantně zvýšilo a zajištění kybernetické bezpečnosti by bylo ohroženo. Z tohoto důvodu jsou požadované informace i v rámci Digitální informační agentury (dále jen „*DIA*“) dostupné pouze pro oprávněné zaměstnance DIA a jejich konkrétně specifikované dodavatele, případně další orgány, které by měly na poskytnutí právní důvod (například Police ČR). Jinými slovy, požadované informace nejsou z důvodu předcházení potenciálním hrozbám běžně přístupné a DIA je tímto způsobem chrání.

16. Bezpečností audit ISDS pak obsahuje bezpečnostní opatření vydané podle zákona o kybernetické bezpečnosti. Zveřejněním těchto informací by mohlo dojít k ohrožení takového opatření, neboť účinnost opatření by mohla být v důsledku zpřístupnění snížena. Znalost bezpečnostních opatření uvedených v bezpečnostním auditu ISDS může vést ke zvýšení rizika kybernetického útoku, jelikož potenciálnímu útočníkovi bude umožněno bezpečnostní opatření obejít.

17. V souvislosti s aktuální judikaturou musí povinné osoby provést u všech zákonných důvodů test proporcionality. Judikaturou byla dovozena základní kritéria tohoto posuzování, kdy je třeba zohlednit vhodnost, potřebnost a porovnat závažnost obou v kolizi stojících základních práv. K otázce vhodnosti, tedy zda lze tímto postupem docílit ochrany kybernetické bezpečnosti, žalovaný uzavřel, že jednoznačně ano. Naopak poskytnutí požadovaných informací má potenciál tuto bezpečnost ohrozit. K otázce potřebnosti, tedy zda by cíle nemohlo být dosaženo bez zasažení do základních práv a svobod, žalovaný uvedl, že nikoliv. Jakmile by byly jednou požadované informace veřejné, šlo by ISDS ochránit pouze velmi obtížně, resp. tento cíl by byl za stávající konfigurace téměř nemožný. K otázce poměřování závažnosti obou v kolizi stojících základních práv žalovaný uzavřel, že informace, které o systému datových schránek mohly být poskytnuty, poskytnuty byly.

18. Poskytnuty nebyly pouze odpovědi na otázky č. 3., 4., 8. a částečně 9., kde bylo vyhodnoceno, že jejich poskytnutí není z bezpečnostních důvodů možné. K omezení práva na informace bylo tedy přistoupeno pouze v minimálním rozsahu, a to tam, kde bylo nebezpečí ohrožení systému kritické infrastruktury vyhodnoceno jako vysoké. Není možné nahradit omezení práva na informace jiným opatřením, které umožní uchránit zájem na bezpečnosti ISDS. V tomto rozsahu opatření spočívající v omezení práva na informace je rovněž vhodné (způsobilé k naplnění ochrany právem chráněného zájmu) a při zohlednění povahy a významu ISDS, jakož i zvýšeném zájmu na jeho bezpečnosti, je proto třeba jej upřednostnit před realizací práva na informace. Poskytnutí požadovaných informací by ve vzájemné propojenosti oslabily jednotlivé prvky kritické infrastruktury, neboť by žalobkyně jako žadatel, resp. veřejnost, po zveřejnění poskytnutých informací podle § 5 odst. 3 InfZ věděli o potenciálních rizicích zabezpečení datových schránek. Takovéto informace nemůže povinný subjekt poskytnout.

19. Žalovaný dále upozornil na nový § 11 odst. 1 písm. f) InfZ, na základě něhož může povinný subjekt omezit poskytnutí informace, pokud „*její poskytnutí významně nebo přímo ohrožuje ochranu kritické infrastruktury*“. Podle názoru žalovaného je výše uvedený důvod pro odmítnutí požadované informace možno využít i přesto, že předmětná žádost byla podána dne 31. 12. 2022. Přechodné ustanovení čl. II zákona č. 241/2022 Sb. totiž konstatuje, že „*žádost o poskytnutí informace podaná přede dnem nabytí účinnosti tohoto zákona se vyřizuje podle zákona č. 106/1999 Sb., ve znění účinném přede dnem nabytí účinnosti tohoto zákona*“. Novela InfZ nabyla účinnosti dne 1. 9. 2022, zatímco žádost byla podána až dne 31. 12. 2022. Novela InfZ totiž použití dosavadního znění InfZ váže na nabytí účinnosti novely InfZ, přičemž z čl. VIII novely InfZ jasně plyne, že „*tento zákon nabývá účinnosti dnem následujícím po dni jeho vyhlášení …*“. V daném případě je tedy zapotřebí postupovat podle InfZ platného a účinného v době vydání rozhodnutí.

20. Žalobkyně reagovala **replikou**, v níž uvedla, že nezpochybňuje, že žalovaný mohl určité informace odmítnout z bezpečnostních důvodů poskytnout. V žádném případě se to ale netýká drtivé většiny informací, které běžně obsahují požadované dokumenty. Žalovaný se snaží navodit dojem, že byly požadovány informace jako přístupová hesla, zabezpečovací kódy apod., což není pravdou a žalobkyni nikdy nenapadlo takové informace požadovat.

21. Žalobkyně ani nepolemizuje s tím, že v rámci výsledků auditů mohou rovněž existovat informace, které mohou systém ohrožovat, konkrétně zjištěné nedostatky v zabezpečení, které se nepodařilo dosud odstranit. Paušální odmítnutí poskytnutí výsledků auditů by ovšem bylo adekvátní pouze tehdy, kdyby všechny audity zjistily nedostatky ohrožující bezpečnost systémů a současně žádné z těchto nedostatků nebyly odstraněny. To je tvrzení, s nímž by se neztotožnil ani žalovaný, a nevěří mu ani žalobkyně. Připomněla, že první bezpečnostní audit, o jehož konání poskytl žalovaný informace, byl proveden společností KPMG v lednu 2018. Zjištěné nedostatky už by tak měly být po této dlouhé době odstraněny. Ostatně šlo by pak o tak důležitou informaci pro občany, jejichž osobní údaje by byly v takových informačních systémech v ohrožení, že i v tomto hypotetickém případě by převážilo právo na informace o naprosto nevyhovujícím stavu takového informačního systému i nekompetentnosti osob, které ho mají na starost.

22. Žalobkyně upozornila, že hodnocení žalovaného k otázce aplikovatelnosti § 11 odst. 1 písm. f) InfZ je chybné. V souladu s čl. II odst. 1 zákona č. 241/2022 Sb. platí, že žádost o poskytnutí informace podaná přede dnem nabytí účinnosti tohoto zákona se vyřizuje podle InfZ ve znění účinném přede dnem nabytí účinnosti tohoto zákona. Žádost o

informace byla podána dne 31. 12. 2022. Nabytí účinnosti novely InfZ, pokud jde o účinnost čl. I. bod 23, který do něj vnesl § 11 odst. 1 písm. f), došlo v souladu s čl. VII písm. a) až dne 1. 1. 2023. Není tedy pravda, že bylo ustanovení aplikovatelné na předmětnou žádost.

III.
Posouzení žaloby

23. Městský soud v Praze (dále jen „*soud*“) ověřil, že žaloba byla podána včas, osobou k tomu oprávněnou, po vyčerpání řádných opravných prostředků a splňuje všechny formální náležitosti na ni kladené. Soud přezkoumal žalobou napadené rozhodnutí i řízení, které mu předcházelo, v rozsahu žalobních bodů, kterými je vázán, přitom vycházel ze skutkového a právního stavu v době vydání rozhodnutí podle § 75 odst. 1 a 2 zákona č. 150/2002 Sb., soudního řádu správního, ve znění pozdějších předpisů (dále jen „*s. ř. s.*“). Vady napadeného rozhodnutí, ke kterým by byl povinen přihlédnout z moci úřední, soud u napadeného rozhodnutí neshledal. Soud rozhodl o věci bez nařízení jednání podle § 51 odst. 1 s. ř. s., neboť žalobkyně s takovým postupem souhlasila a žalovaný se k možnosti takového postupu ve lhůtě stanovené soudem nevyjádřil, a má se tedy za to, že s takovým postupem souhlasí.

24. Na základě prokázaného skutkového stavu věci dospěl soud k závěru, že žaloba není důvodná.

25. Soud se nejprve zabýval žalobkyní tvrzenou nepřezkoumatelností napadeného rozhodnutí (**první žalobní bod**). Pokud by takováto námitka byla důvodná, bránila by uvedená vada věcnému posouzení napadeného rozhodnutí.

26. Soud připomíná, že nepřezkoumatelnost správního rozhodnutí spočívá podle § 76 odst. 1 písm. a) s. ř. s. v nesrozumitelnosti nebo nedostatku důvodů rozhodnutí, přičemž nepřezkoumatelnost rozhodnutí správního orgánu pro nesrozumitelnost předchází případné nepřezkoumatelnosti pro nedostatek jeho důvodů; důvody rozhodnutí lze zkoumat toliko u rozhodnutí srozumitelných (rozsudek Nejvyššího správního soudu ze dne 23. 7. 2008, č. j. 3 As 51/2007-84). Za nesrozumitelnost rozhodnutí soudy považují například případy, kdy odůvodnění nedává smysl, který by svědčil o skutkových a právních důvodech, které vedly správní orgán k vydání rozhodnutí (rozsudek Nejvyššího správního soudu ze dne 24. 9. 2003, č. j. 7 A 547/2002-24); pro rozpor výroku s odůvodněním (rozsudek Nejvyššího správního soudu ze dne 12. 12. 2003, č. j. 2 Ads 33/2003-78) či pro výrok, který nemá oporu v zákoně (rozsudek Nejvyššího správního soudu ze dne 29. 5. 2003, č. j. 7 A 181/2000-29), nebo není-li rozhodnutí rozčleněno na výrok a odůvodnění, pročež není zřejmé, zda správní orgán rozhodl o všech návrzích účastníka řízení (rozsudek Vrchního soudu v Praze ze dne 21. 10. 1994, č. j. 6 A 63/93-22).

27. Rozhodnutí je nepřezkoumatelné pro nedostatek důvodů, jestliže z jeho odůvodnění není seznatelné, proč správní orgán považuje námitky účastníka za liché, mylné nebo vyvrácené, které skutečnosti vzal za podklad svého rozhodnutí, proč považuje skutečnosti tvrzené účastníkem za nerozhodné, nesprávné nebo jinými řádně provedenými důkazy vyvrácené, podle které právní normy rozhodl a jakými úvahami se řídil při hodnocení důkazů. Nepřezkoumatelnost rozhodnutí pro nedostatek důvodů musí být vykládána ve svém skutečném smyslu, tj. jako nemožnost přezkoumat určité rozhodnutí pro nemožnost zjistit v něm jeho obsah nebo důvody, pro které bylo vydáno (viz usnesení rozšířeného

senátu Nejvyššího správního soudu ze dne 19. 2. 2008, č. j. 7 Afs 212/2006-76). Není přípustné institut nepřezkoumatelnosti libovolně rozšiřovat a vztáhnout jej i na případy, kdy se správní orgán podstatou námitky účastníka řízení řádně zabývá a vysvětlí, proč nepovažuje argumentaci účastníka za správnou, byť výslovně v odůvodnění rozhodnutí nereaguje na všechny myslitelné aspekty vznesené námitky a dopustí se dílčího nedostatku odůvodnění. Zrušení rozhodnutí pro nepřezkoumatelnost je vyhrazeno těm nejzávažnějším vadám rozhodnutí, kdy pro absenci důvodů či pro nesrozumitelnost skutečně nelze rozhodnutí meritorně přezkoumat.

28. S ohledem na zásadu jednotnosti správního řízení je nutné napadená rozhodnutí posuzovat jako celek (viz usnesení rozšířeného senátu Nejvyššího správního soudu ze dne 12. 10. 2004, č. j. 5 Afs 16/2003-56, či přiměřeně rozsudek Nejvyššího správního soudu ze dne 27. 2. 2013, č. j. 6 Ads 134/2012-47). Napadená rozhodnutí posoudil soud optikou výše uvedené judikatury a dospěl k závěru, že rozhodnutí nepřezkoumatelná nejsou. Z jejich odůvodnění je zřejmé, z jakého skutkového stavu správní orgány vyšly, jak vyhodnotily pro věc rozhodné skutkové okolnosti a jak je následně právně posoudily. Rozhodnutí jsou řádně odůvodněna a jsou plně srozumitelná. Úvahy ve vztahu k žalobkyni jsou individualizovány. To ostatně dokládá i skutečnost, že se k jednotlivým závěrům správních orgánů v její věci žalobkyně vyjadřuje a polemizuje s nimi. Napadená rozhodnutí tak obsahují veškeré náležitosti stanovené § 68 odst. 2 správního řádu.

29. Žalobní námitka není důvodná.

30. Dále soud přistoupil k posouzení **druhého žalobního bodu**.

31. K tomu předně uvádí, že v projednávané věci je mezi účastníky spor o poskytnutí informace – dokumentů na základě informačního zákona (dokumentace Enteprise Architecture, dokumentace bezpečnostní architektury, bezpečnostní politiky a bezpečnostních požadavků dodavatele, seznam software a hardware využitého v architektuře ISDS, včetně vybavení s oprávněním přístupu do ISDS), včetně externích auditů ISDS a obslužného vybavení, a včetně auditů provedených u zpracovatelů podílejících se na provozu systému ISDS.

32. Právo na informace je garantováno každému na základě čl. 17 odst. 4 usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdější předpisů (dále jen „*LZPS*“). Provádění tohoto základního práva zabezpečuje informační zákon, jenž je vystavěn na principu obecné povinnosti poskytovat veškeré informace týkající se působnosti povinných subjektů s taxativně vymezenými výlukami z této povinnosti.

33. Dle Nejvyššího správního soudu „je *smyslem práva na informace kontrola činnosti veřejné správy, mj. též kontrola vynakládání veřejných prostředků a hospodaření s veřejným majetkem*“ (rozsudek Nejvyššího správního soudu ze dne 7. 5. 2008, č. j. 1 As 17/2008-67, Sb. NSS č. 1627/2008) a „*poskytování informací o činnosti orgánů veřejné moci je v našem civilizačním prostoru obecným standardem demokratických právních států, který logicky vyžaduje jisté finanční zatížení orgánů veřejné správy*“, jakož i to, že „*povinný subjekt není oprávněn jakkoli zkoumat a zabývat se otázkou účelnosti a důvodnosti žadatelovy žádosti či jeho motivy*“ (rozsudek Nejvyššího správního soudu ze dne 27. 6. 2007, č. j. 6 As 79/2006-58, Sb. NSS č. 1342/2007).

34. Při posouzení věci vycházel soud z následující právní úpravy.

35. Podle čl. 17 odst. 4 LZPS lze „*svobodu projevu a právo vyhledávat a šířit informace omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti*“.

36. Dle § 11 odst. 1 písm. d) InfZ může „*povinný subjekt omezit poskytnutí informace, pokud: její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku*“.

37. Dle § 12 InfZ „*všechna omezení práva na informace provede povinný subjekt tak, že poskytne požadované informace včetně doprovodných informací po vyloučení těch informací, u nichž to stanoví zákon. Právo odepřít informaci trvá pouze po dobu, po kterou trvá důvod odepření. V odůvodněných případech povinný subjekt ověří, zda důvod odepření trvá*“.

38. Dle § 15 odst. 1 InfZ „*pokud povinný subjekt žádosti, byť i jen zčásti, nevyhoví, vydá ve lhůtě pro vyřízení žádosti rozhodnutí o odmítnutí žádosti, popřípadě o odmítnutí části žádosti, s výjimkou případů, kdy se žádost odloží*“.

39. Podle § 10a zákona o kybernetické bezpečnosti se „*informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, podle předpisů upravujících svobodný přístup k informacím neposkytují*“.

40. Podle obsahu správního spisu bylo v prvostupňovém rozhodnutí odmítnutí poskytnutí vybrané dokumentace odůvodněno ochranou kybernetické bezpečnosti. Správní orgán I. stupně a žalovaný zdůvodnili odepření poskytnutí vybraných informací ochranou kybernetické bezpečnosti podle § 10a zákona o kybernetické bezpečnosti ve spojení s § 11 odst. 1 písm. d) InfZ.

41. Správní orgán I. stupně uvedl jako důvod odmítnutí poskytnutí informací k jednotlivým bodů žádosti žalobkyně v prvostupňovém rozhodnutí následující.

42. K bodům 3., 4. a 8. uvedl, že v případě poskytnutí žalobkyní požadovaných dokumentů by mohlo dojít k ohrožení účinnosti bezpečnostních opatření a zajišťování kybernetické bezpečnosti a případný útočník by uvedené informace mohl využít k lepšímu zacílení svých útoků. U bodu 8 správní orgán I. stupně dodal, že software a hardware jsou podpůrná aktiva ISDS, opatření spadá do kategorie řízení aktiv (§ 5 odst. 2 písm. f) zákona o kybernetické bezpečnosti), proto by v případě poskytnutí informace mohlo dojít k ohrožení účinnosti bezpečnostních opatření a útočník by uvedené informace mohl využít k lepšímu zacílení svých útoků – věděl by, které softwarové nebo hardwarové prvky jsou přístupné online a lépe by tak zacílil své útoky. Zároveň by znal typy a značky těchto zařízení, tedy by si snadněji dohledal jejich případné zranitelnosti.

43. K bodu 9. správní orgán I. stupně uvedl, že přehled auditů ISDS provedených provozovatelem za období 2018 až 2022 zasílá samostatnou přílohou. Audity činěné Národním úřadem pro kybernetickou bezpečnost (NÚKIB) či Nejvyšším kontrolním úřadem (NKÚ) jsou zveřejňované prostřednictvím jejich úřední desky, tudíž je správní orgán I. stupně nemá k dispozici. Vlastní závěry auditu však poskytnout nelze, jelikož jejich zveřejnění může ohrozit účinnost navržených bezpečnostních opatření, nebo by mohly sloužit k lepšímu zacílení kybernetických útoků.

44. Uvedené důvody podpořil v napadeném rozhodnutí též žalovaný.

45. K bodu 3. a 4. žalovaný připomněl, že účinnost jakéhokoliv bezpečnostního opatření (byť preventivní povahy, jako např. klasifikace informací označením jejich ochrany) by byla přímo ohrožena, pokud by takové informace, v rozporu s bezpečnostním opatřením, byly zpřístupněny. Doplnil, že za situace, kdy správci systémů kritické informační infrastruktury jsou zároveň povinnými subjekty podle InfZ, a kdy zároveň roste počet kybernetických útoků, je bezpochyby zapotřebí přistoupit k opatřením i v obecnější rovině v oblasti zajišťování kybernetické bezpečnosti. Potenciální útočník proto nesmí mít možnost získat informace ohrožující kybernetickou bezpečnost s odkazem na žádost o informaci. Informací, jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, by podle důvodové zprávy mohla být např. schémata, plány, technické specifikace (topologie sítě), konfigurační parametry či havarijní plány. Požadované informace by bylo možné využít k zacílení kybernetického útoku a způsobení závažnějších následků kybernetického útoku. Riziko kybernetického útoku by se tedy razantně zvýšilo a zajištění kybernetické bezpečnosti by bylo ohroženo. Podle žalovaného neměl správní orgán I. stupně možnost uvážení, zda v daném případě poskytne či neposkytne požadované informace. Vzhledem k tomu, že ISDS je systémem kritické informační infrastruktury, je právními předpisy požadována maximální míra zabezpečení.

46. K bodu 8. žalovaný doplnil, že v tomto případě je bezpečnostním rizikem poskytnout požadovanou informaci, jelikož její specifikace sama o sobě může naznačit koncepci systémové architektury, a tím snížit nastavená bezpečnostní opatření systému, která mají za úkol zajistit požadovanou úroveň zabezpečení daného systému. Z tohoto důvodu je nezbytné zabezpečit, aby software a hardware neměly žádné zranitelnosti. Případné poskytnutí požadované informace by tak bylo zcela v rozporu s pravidly nastavené bezpečnostní politiky. S ohledem na významnost systému ISDS a citlivost údajů, které jsou v rámci systému zpracovávány, musí být pravidla nastavené bezpečnostní politiky prioritou nejen pro provozovatele ISDS, ale i uživatele. I zde platí, že pokud jsou případnému útočníkovi poskytnuty seznamy toho, co je v daném systému využíváno, tak dochází k usnadňování práce útočníka a navyšování rizika útoků na ISDS (kvůli lepšímu zacílení útoků). Není tedy jakkoliv žádoucí usnadňovat případnému útočníkovi práci, kterou by se zjišťováním těchto informací měl. Stejně tak není žádoucí zvyšovat, byť sebemenší, riziko prolomení.

47. Soud se s výše uvedenou argumentací správních orgánů obou stupňů ztotožňuje a uzavírá, že došlo k dostatečnému vymezení důvodů pro neposkytnutí žalobkyní požadovaných informací, a to z hlediska relevantní právní úpravy a též ve smyslu relevantní judikatury správních soudů. Soud tak považuje odmítnutí poskytnutí informace za souladné s právními předpisy, za náležitě a dostatečným způsobem odůvodněné a rovněž za srozumitelně objasněné, v čem je spatřováno naplnění všech podmínek k odepření konkrétních požadovaných informací (dokumentací).

48. V projednávané věci spadají žalobkyní požadované informace, resp. dokumenty, pod dikci § 10a zákona o kybernetické bezpečnosti. Předmětné ustanovení bylo do zákona o kybernetické bezpečnosti vloženo novelou účinnou od 1. 8. 2017. Dle důvodové zprávy k novelizačnímu zákonu „*stávající úprava* (před 1. 8. 2017, pozn. soudu) *obsažená v § 11 odst. 4 zmiňovaného zákona však cílí pouze na úzký okruh informací, konkrétně na informace z evidence incidentů vedené podle § 9 zákona o kybernetické bezpečnosti.* […] *Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných*

informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout. Z tohoto důvodu se předkladatel rozhodl [...] *pro doplnění výjimky z povinnosti poskytovat informace na základě zákona o svobodném přístupu k informacím o údaje, které se týkají zajišťování kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti*“ (blíže viz Komentář k § 10a zákona o kybernetické bezpečnosti, In: Maisner, M. – Vlachová, B, *Zákon o kybernetické bezpečnosti. Komentář*, Wolters Kluwer: ASPI, právní stav k 1. 2. 2020).

49. Důvodová zpráva dále uvádí, že jde o „*informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle tohoto zákona. Těmito opatřeními jsou varování, reaktivní opatření a ochranná opatření. Jedná se o instituty, jejichž zveřejnění ne vždy může ohrozit jejich účinnost, případně mít dopad na zajišťování kybernetické bezpečnosti, z tohoto důvodu jsou v návrhu ustanovení § 10a uvedeny zvlášť. Předkladatel návrhu zákona se domnívá, že toto omezení práva na informace je plně v souladu s čl. 17 odst. 4 LZPS, když dospěl k názoru, že v oblasti kybernetické bezpečnosti, která hraje v oblasti bezpečnosti státu stále důležitější roli, převážil požadavek na zajištění bezpečnosti státu a veřejné bezpečnosti, přičemž považuje za nutné konstatovat, že povinný subjekt bude vždy při rozhodování o žádosti o poskytnutí informací povinen posoudit, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti a pečlivě v daném případě zvažovat potřebu omezení práva na informace*.“

50. Dle doporučení NÚKIB k § 10a zákona o kybernetické bezpečnosti ze dne 29. 1. 2019 [dostupné na: https://nukib.gov.cz/download/publikace/podpurne_materialy/Doporuceni-NUKIB_ustanoveni-10a_v1.2.pdf, a v rozšířené a aktualizované verzi ze dne 22. 12. 2022 na: https://nukib.gov.cz/download/publikace/podpurne_materialy/Doporuceni_Poskytovani-informaci_v2.1.pdf] se „*při posuzování, zda informace poskytnout či nikoliv, je nezbytné zvážit, které informace jsou z hlediska zachování kybernetické bezpečnosti natolik důvěrné, že by jejich vyzrazením mohlo dojít k jejímu narušení. Taková informace by také měla z pohledu důvěrnosti odpovídat úrovni „Vysoká“ nebo „Kritická“ podle přílohy č. 1 vyhlášky o kybernetické bezpečnosti. Pokud by zpřístupněním takové informace mohlo dojít k narušení kybernetické bezpečnosti, je podle názoru NÚKIB vhodné uvažovat o použití § 10a zákona kybernetické bezpečnosti a takovou informaci neposkytnout. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní dokumentaci*.“

51. NÚKIB se v doporučení vyjadřuje i k soudnímu přezkumu, kdy upozorňuje, že „*při případném soudním řízení o oprávněnosti neposkytnutí informace podle § 10a zákona o kybernetické bezpečnosti jsou předmětem soudního přezkumu zejména důvody neposkytnutí informací, tedy také to, zda informace naplní definici tohoto ustanovení zákona. Argumentace prostřednictvím klasifikace informací při hodnocení aktiv se tak prima vista jeví jako nezbytná*.“

52. Omezení práva na informace uvedené v § 10a zákona o kybernetické bezpečnosti se vztahuje na tři druhy informací: (1) informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti; (2) jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti, (3) které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila.

53. V aktuálně posuzované věci jde dle obsahu napadených rozhodnutí o neposkytnutí informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti. Opatřeními jsou podle § 11 odst. 2 písm. a) až c) zákona o kybernetické bezpečnosti: varování; reaktivní opatření; ochranné opatření. K těmto důvodům pro odmítnutí poskytnutí informace povinný subjekt uvádí, dle jakých kritérií se posuzuje hodnota aktiv, tedy informací.

54. Dle důvodové zprávy a doporučení NÚKIB ve vztahu k § 11 odst. 1 písm. d) InfZ „*další konkretizací navržené výjimky jsou parametry významného nebo přímého účinku posuzované informace. Významné ohrožení účinnosti by mělo být takové, které by samo o sobě vedlo k nemožnosti zajistit chráněný účel.* (...) *Ochranu by měly získat jen ty informace, u kterých lze prokázat kombinaci uvedených rysů – poskytnutí by významně a přímo ohrozilo účinnost bezpečnostního opatření, například v případě kybernetické bezpečnosti kybernetickou bezpečnost a bezpečnost sítí a informačních systémů. Dalším vymezujícím parametrem je nezbytnost opatření. Nebylo by totiž přiměřené, pokud by se umožnilo rozsáhlé a neobvyklé utajování informací jen proto, že si některý povinný subjekt vytvořil natolik mimořádné, komplikované či sofistikované bezpečnostní opatření, které již není nezbytné, ale jehož funkce je na mimořádném rozsahu utajování závislá. Vždy totiž existuje určitá úměrnost mezi účinností bezpečnostního opatření a tím, do jaké míry jsou o něm dostupné informace – čím méně dostupných informací, tím vyšší účinnost.* (...) *Chránit lze toliko nezbytná opatření, což mj. plyne z ústavní kautely v čl. 17 odst. 4 Listiny, kde se přístup k informacím umožňuje omezit jen potud, pokud „jde o opatření v demokratické společnosti nezbytná*“.“

55. K omezení poskytnutí informace podle § 11 odst. 1 písm. d) InfZ správní orgán I. stupně nejprve citoval zákonnou právní úpravu a poté provedl stručné posouzení a zdůvodnění toho, proč nemůže žalobkyní požadované dokumenty poskytnout, a to ve vztahu k § 10a zákona o kybernetické bezpečnosti. Žalovaný závěry správního orgánu I. stupně podpořil a dále doplnil.

56. Správní orgány obou stupňů přitom především zaujaly názor, že veřejný zájem na informování uživatelů o zabezpečení datových schránek – tedy zachování ústavně zaručeného práva na informace, není vyšší než ochrana informací chráněných dle zákona o kybernetické bezpečnosti, konkrétně zájmu na ochraně kybernetické bezpečnosti datových schránek.

57. Soud souhlasí se závěrem správních orgánů, že v daném případě je potenciální poskytnutí dokumentace bezpečnostní architektury informačního systému datových schránek, případně provedených auditů, takovou informací, která může ohrozit funkčnost informačního systému datových schránek, přičemž lze toto nebezpečí vyhodnotit jako významné nebo přímo ohrožující, kdy by došlo k poskytnutí informací popisující nedostatky daného systému, neboť by na základě této informace žadatel mohl získat přehled o obecně zranitelných místech tohoto prvku kritické informační infrastruktury. Je třeba mít na zřeteli, že je ISDS systémem kritické informační infrastruktury (mj. podle zákona o kybernetické bezpečnosti, zákona č. 240/2000 Sb., o krizovém řízení, a nařízení vlády č. 432/2010 Sb.), a právními předpisy je požadována maximální míra jeho zabezpečení, pročež riziko ohrožení účinnosti bezpečnostních opatření je v případě poskytnutí požadovaných informací významné a přímé.

58. Soud pak vzhledem k povaze dokumentací vyžadovaných žalobkyní nepřisvědčil ani její stěžejní žalobní námitce, že správní orgán I. stupně mohl poskytnout alespoň část

dokumentace vyžadované žalobkyní pod body 3., 4. a 8. její žádosti. Je tomu tak proto, že poskytnutí pouze částí požadovaných dokumentací není vzhledem k charakteru požadovaných dokumentů možné.

59. Soud připomíná že žalobkyně požadovala: kompletní dokumentaci Enterprise Architecture, včetně všech relevantních příloh; kompletní dokumentaci bezpečnostní architektury, dokumentaci bezpečnostní politiky dle § 5 odst. 2 písm. c) zákona o kybernetické bezpečnosti a dále dokumentaci bezpečnostních požadavků na dodavatele dle § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti; seznam software a hardware, který je využit v architektuře ISDS, včetně vybavení s oprávnění přístupu do ISDS (počítače administrátorů atd.), a vyžadoval online aktivaci, a nebo má povolenu online aktualizaci; seznam všech externích auditů provedených na ISDS a obslužném vybavení (pokud byly provedeny) včetně auditů provedených u zpracovatelů podílejících se na provozu systému ISDS, s definicí rozsahu auditu, jeho závěry a doložením kvalifikace auditora k dané odbornosti.

60. Soud souhlasí se žalovaným, že poskytnutí, byť jen části žalobkyní požadovaných informací, tj. části výše uvedených dokumentací či jen vybraných informací a dokumentů z nich, by ve vzájemné propojenosti oslabilo jednotlivé prvky kritické infrastruktury, neboť by tím byla zveřejněna potenciální rizika zabezpečení datových schránek, což představuje vysoké bezpečnostní riziko. I pouhé zpřístupnění vybraných částí architektury IT systému (Enterprise Architecture) a bezpečnostní architektury datových schránek, včetně využívaného software a hardware v architektuře ISDS, by představovalo vysoké ohrožení zabezpečení celé bezpečnostní architektury systému datových schránek.

61. K obdobným závěrům přitom došel již žalovaný v napadeném rozhodnutí, kde uvedl, že „*lze, s ohledem na povahu výše požadovaných informací (pod bodem 3 a 4), dovodit významné i přímé ohrožení účinnosti bezpečnostního opatření a předpisů v oblasti kybernetické bezpečnosti. To zejména z toho důvodu, že účinnost opatření v oblasti kybernetické bezpečnosti se úměrně snižuje s tím, nakolik je toto opatření známo. I proto správní orgán I. stupně neposkytl žádnou část požadovaných dokumentů*,“ a dále ve vztahu k bodu 8, že specifikace software a hardware v architektuře ISDS „*sama o sobě může naznačit koncepci systémové architektury, a tím snížit nastavená bezpečnostní opatření systému, která mají za úkol zajistit požadovanou úroveň zabezpečení daného systému. Z tohoto důvodu je nezbytné zabezpečit, aby software a hardware neměly žádné zranitelnosti. Případné poskytnutí požadované informace by tak bylo zcela v rozporu s pravidly nastavené bezpečnostní politiky*.“

62. V uvedeném případě se jedná o ochranu informací, u kterých lze prokázat, že by jejich poskytnutí významně a přímo ohrozilo účinnost bezpečnostního opatření, konkrétně kybernetickou bezpečnost a bezpečnost sítí a informačních systémů. Proto nebyly dány podmínky ani pro zpřístupnění, byť jen části požadovaných informací, kterých se žalobkyně domáhala. Správní orgány tak nepochybily, pokud 3., 4. a 8. bodu žádosti žalobkyně nevyhověly, a to ani poskytnutím jen části vyžadovaných dokumentací. Jinak vzhledem k vysoké důvěrnosti vyžadovaných informací a potřebě zachování celistvé ochrany systému postupovat nemohly.

63. Úvahy správních orgánů obou stupňů podporuje též Vyhláška č. 82/2018 Sb., podle které předmětné informace, jako aktiva označená z hlediska důvěrnosti stupněm „vysoká“, nejsou veřejně přístupná a jejich ochrana, považovaná za velmi důležitou, je vyžadována právními předpisy, přičemž vyžadují ochranu z hlediska integrity. Závěr o potřebě zvýšené

ochrany předmětných informací podporuje též uplatňování metody zabezpečení tzv. Security through obscurity (bezpečnost skrze neznalost), kdy z logiky věci zveřejnění jen části informací o kritické infrastruktuře může usnadnit nalezení chyb v systému a vést tak k jeho snazšímu a rychlejšímu prolomení.

64. K bodu 9 žádosti, kde bylo žádosti žalobkyně částečně vyhověno, pak soud v souladu se závěrem správního orgánu I. stupně uvádí, že žalobkyni bylo poskytnuto maximum možných informací tak, aby nebylo ohroženo zabezpečení ISDS. Byly by to totiž právě závěry auditu NÚKIB či NKÚ, které by odhalovaly konkrétní slabiny a rizika daného systému, resp. řešené technické problémy. Uvedené informace by proto bezpochyby mohly představovat potenciální cíle pro zaměření kybernetických útoků. Z povahy informací obsažených v uvedených auditech a jejich vztahu k celistvosti a obranyschopnosti systému ISDS je tak, a to ani v omezené míře, poskytnout nelze. Žalobkyni tak v tomto bodu její žádosti byla poskytnuta informace v nejširším možném rozsahu.

IV.
Závěr a rozhodnutí o nákladech řízení

65. Na základě shora uvedeného soud dospěl k závěru, že žaloba není důvodná, proto ji podle § 78 odst. 7 s. ř. s. zamítl.

66. O nákladech řízení soud rozhodl podle § 60 odst. 1 s. ř. s., podle kterého má účastník, který měl ve věci plný úspěch, právo na náhradu nákladů řízení před soudem, které důvodně vynaložil, proti účastníkovi, který ve věci úspěch neměl. Ve věci měl plný úspěch žalovaný, kterému v řízení žádné náklady nad rámec jeho běžných činností nevznikly. Soud proto rozhodl, že žádný z účastníků nemá právo na náhradu nákladů tohoto řízení.

Poučení:

Proti tomuto rozhodnutí lze podat kasační stížnost ve lhůtě dvou týdnů ode dne jeho doručení. Kasační stížnost se podává ve dvou (více) vyhotoveních u Nejvyššího správního soudu, se sídlem Moravské náměstí 6, Brno. O kasační stížnosti rozhoduje Nejvyšší správní soud.

Lhůta pro podání kasační stížnosti končí uplynutím dne, který se svým označením shoduje se dnem, který určil počátek lhůty (den doručení rozhodnutí). Připadne-li poslední den lhůty na sobotu, neděli nebo svátek, je posledním dnem lhůty nejblíže následující pracovní den. Zmeškání lhůty k podání kasační stížnosti nelze prominout.

Kasační stížnost lze podat pouze z důvodů uvedených v § 103 odst. 1 s. ř. s. a kromě obecných náležitostí podání musí obsahovat označení rozhodnutí, proti němuž směřuje, v jakém rozsahu a z jakých důvodů jej stěžovatel napadá, a údaj o tom, kdy mu bylo rozhodnutí doručeno.

V řízení o kasační stížnosti musí být stěžovatel zastoupen advokátem; to neplatí, má-li stěžovatel, jeho zaměstnanec nebo člen, který za něj jedná nebo jej zastupuje,

vysokoškolské právnické vzdělání, které je podle zvláštních zákonů vyžadováno pro výkon advokacie.

Soudní poplatek za kasační stížnost vybírá Nejvyšší správní soud. Variabilní symbol pro zaplacení soudního poplatku na účet Nejvyššího správního soudu lze získat na jeho internetových stránkách: www.nssoud.cz.

Praha 17. duben 2024

JUDr. Slavomír Novák v.r.

předseda senátu

Shodu s prvopisem potvrzuje J. V.