ČESKÁ REPUBLIKA

ROZSUDEK JMÉNEM REPUBLIKY

Městský soud v Praze rozhodl v senátě složeném z předsedy JUDr. Ladislava Hejtmánka a soudkyň JUDr. Hany Kadaňové, Ph.D. a Mgr. Hany Janotové ve věci

žalobce: **J. C.**
bytem X

proti

žalovanému: **Ministerstvo pro místní rozvoj**
sídlem Staroměstské náměstí 6, Praha

o žalobě proti rozhodnutí žalovaného ze dne 24. října 2025, č. j. MMR-70418/2025-31,

takto:

I. Rozhodnutí Ministerstva pro místní rozvoj ze dne 24. října 2025, č. j. MMR-70418/2025-31, se ruší, a věc se vrací žalovanému k dalšímu řízení.

II. Žalovaný je povinen žalobci zaplatit náhradu nákladů řízení tvořených zaplaceným soudním poplatkem ve výši 3 000 Kč, a to do 30 dnů od právní moci tohoto rozsudku.

Odůvodnění:

I. Vymezení věci

[1] Žalobce podal dne 14. 2. 2025 žádost o poskytnutí zpráv z provedeného penetračního testování systémů Digitálního stavebního řízení (dále též „*DSŘ*“), a to k Ministerstvu pro místní rozvoj (dále též „*povinný subjekt*“ nebo „*žalovaný*“). Podanou žalobou brojí proti neposkytnutí informace pod č. 4 žádosti, kde se domáhal „*poskytnutí výsledných zpráv z penetračního testování systémů digitálního stavebního řízení, zpracovaných společnostmi ESET a DCIT (zakázky č. VZ/2024/034/1064 a VZ/2024/034/1074)*“.

[2] Žádost byla dne 25. 4. 2025 povinným subjektem částečně odmítnuta rozhodnutím č. j. MMR-33456/2025-31. V rámci jeho vydání nebyla dodržena zákonná lhůta pro vydání rozhodnutí. Žalobce nejdříve musel neúspěšně vyčerpat ochranné prostředky proti nečinnosti. Poté musel podat žalobu na ochranu proti nečinnosti ke zdejšímu soudu. V usnesení ze dne 30. 6. 2025, č. j. 17 A 34/2025-32, zdejší soud uvedl, že ke dni podání žaloby byl povinný subjekt nečinný ve věci (řízení bylo zastaveno z důvodu zpětvzetí žaloby, neboť žalovaný po podání nečinnostní žaloby vydal rozhodnutí).

[3] Žalobce následně podal v dané věci rozklad. O něm opět při nedodržení zákonné lhůty rozhodoval ministr pro místní rozvoj, který dané rozhodnutí zrušil a věc vrátil povinnému subjektu k novému projednání. Povinný subjekt byl i nadále nečinný. Ministr pro místní rozvoj ani v tomto případě nic neučinil k odstranění nečinnosti. Žalobce se proto znovu obrátil za zdejší soud. Byl vydán rozsudek ze dne 10. 11. 2025, č. j. 18 A 75/2025-33, kterým byla znovu konstatována nečinnost povinného subjektu.

[4] Žalobce se obával, že povinný subjekt zaujme nečinnostní postoj i „napotřetí“. Z toho důvodu se rozhodl využít možnosti, kterou uvedl Nejvyšší správní soud ve svém rozsudku ze dne 24. 10. 2018, č. j. 7 As 192/2017-35, a podanou žalobou napadl přímo rozhodnutí povinného subjektu ze dne 24. 10. 2025, č. j. MMR-70418/2025-31 /pozn. soudu: proto je v nyní posuzované věci povinným subjektem i žalovaným týž orgán/.

II. Žalobní argumentace

[5] Žalobce se v podané žalobě vymezuje proti tvrzení žalovaného, který odmítl poskytnout jakékoli požadované informace, a to včetně údajů o počtech nalezených zranitelností a informaci o použité metodě testování IT systémů. Dle žalobce není tento postup souladný s ustanovením § 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „*informační zákon*“) a s ustanovením § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „*kybernetický zákon*“).

[6] Žalobce argumentuje zákazem extenzivního výkladu omezení práva na informace a odkazuje na nález Ústavního soudu ze dne 30. 3. 2010, sp. zn. Pl. ÚS 2/10. Dále poukazuje na znění § 12 informačního zákona.

[7] Uvádí, že i v situaci, kdy by zprávy z penetračního testování obsahovaly takové skutečnosti, které by nemohly být zveřejněny z důvodu ochrany před ohrožením bezpečnosti testovaných systémů, není tím ospravedlněno neposkytnutí celého materiálu. Dle žalobce tak žalovaný musí přesně určit, které informace musí být chráněny a anonymizovat je. Současně musí v odůvodnění svého rozhodnutí jejich vyloučení dostatečně odůvodnit.

[8] Žalobce poukazuje na odůvodnění napadeného rozhodnutí, konkrétně na str. 3 a 4. Zdůrazňuje, že ačkoli žalovaný zmiňuje, že redakci požadovaných dokumentů zvažoval, tuto možnost následně vyloučil. Dle žalobce však absentuje uvedení důvodu, proč nebyla redakce možná. Postrádá zdůvodnění, z jakého důvodu nebylo možné poskytnout informaci o tom, „*jakou metodou testování probíhalo (např. OWASP TOP 10), a jaký počet zranitelností v jednotlivých stupních závažnosti (kritická, vysoká, střední, nízká) byl zjištěn*“. Dále žalobce postrádá odůvodnění nemožnosti poskytnout údaje o časovém a personálním rozsahu testování.

[9] Žalobce se vymezuje taktéž vůči odmítnutí poskytnutí těch částí předmětných zpráv, o jejichž detailech se bylo možné dočíst v médiích. Jedná se o informaci o chybě systému, která dávala všem uživatelům možnost prohlédnout si a změnit dokumenty uživatelů jiných. Zároveň se uživatelé mohli do geoportálu územního plánování přihlásit pomocí uhodnutého číselného identifikátoru. Žalobce dodává, že obě tyto zranitelnosti byly již odstraněny, a proto poskytnutí daných informací nemůže vést ke zneužití těchto chyb.

[10] Dle žalobce mohl žalovaný poskytnout také „alespoň rámcové“ údaje o dalších zranitelnostech, které byly taktéž odstraněny. Poskytnutí mohlo být provedeno předně u částí systému, jež nebyly zprovozněny.

[11] Závěrem žalobce odkazuje na rozsudky zdejšího soudu, věnující se otázce kyberbezpečnosti, ve věci 9 A 161/2019 a ve věci 8 A 82/2023.

[12] Z výše uvedených důvodů žalobce navrhuje zrušení napadeného rozhodnutí a uložení povinnosti žalovanému poskytnout požadované informace do 7 dnů od právní moci rozsudku.

III. Shrnutí odůvodnění napadeného rozhodnutí

[13] V rámci odůvodnění napadeného rozhodnutí žalovaný zdůvodnil nemožnost poskytnutí výsledných zpráv z penetračního testovánu systému DSŘ následovně.

[14] Žalovaný se odvolává na odborné stanovisko Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „*NÚKIB*“) a na určení DSŘ za informační systém kritické infrastruktury (položka 534 – Informační systému podporující služby stavebního řízení a územního plánování), které bylo provedeno po meziresortním projednání vládou České republiky. Uvádí, že systém podléhá režimu ochrany dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen „*krizový zákon*“) a dle kybernetického zákona. Poukazuje na povinnost k zajišťování bezpečnostních opatření dle § 5 kybernetického zákona a na omezení možnosti poskytovat informace, jejichž zpřístupněním by mohlo dojít k ohrožení zajišťování kybernetické bezpečnosti dle § 10 téhož zákona.

[15] Popisuje, ze kterých částí se skládají předmětné zprávy z penetračního testování. Jedná se o „*detailní technické popisy nalezených zranitelností, konfigurací a*

přístupových mechanismů, architekturu systému, síťové typologie a rozhraní, popisy využitých metod testování a simulací útoků a doporučení k nápravě a vyhodnocení zbytkového rizika“. Dle žalovaného představují výše uvedené informace citlivé bezpečnostní údaje. V případě jejich zveřejnění by bylo možné odhalit slabiny systému, čímž by byla usnadněna příprava cílených kybernetických útoků. Rovněž by byla ohrožena funkce systému DSŘ, jenž je připojen k dalším státním systémům.

[16] V souvislosti s výše uvedeným žalovaný argumentuje zněním ustanovení § 11 odst. 1 písm. d) informačního zákona. Rovněž uvádí ustanovení § 10a kybernetického zákona, přičemž tento předpis označuje za zvláštní úpravu ve vztahu k informačnímu zákonu, která se vztahuje na veškeré informace týkající se ochrany, bezpečnostních opatření a zranitelností prvků kritické infrastruktury.

[17] Žalovaný dále popisuje, jak prováděl test proporcionality, v jehož rámci zkoumal, zda nelze poskytnout alespoň částečnou informaci ve smyslu § 12 informačního zákona. Nejprve se zabýval zhodnocením celkové citlivosti informací. K tomuto uvádí, že jelikož obsahem předmětné zprávy jsou nejen izolované zranitelnosti, nýbrž i celkový kontext systému (jeho architektura, síťové topologie, nastavení přístupových mechanismů a metodika testování), v důsledku vzájemné propojenosti jednotlivých prvků by i při odstranění detailů o jednotlivých zranitelnostech bylo možné, aby potenciální útočníci zbylé informace (strukturu sítí, typy používaných komponent atd.) použili k rekonstrukci celkového obrazu systému. Tím by bylo možné odhadnout, jaké další slabiny daný systém vykazuje.

[18] Dále se žalovaný zabýval tím, zda by případné redakční úpravy představovaly efektivní řešení. Uvádí, že i při částečné anonymizaci daného dokumentu provedené zakrytím IP adres, názvů serverů a konkrétních CVE by stále nebylo zabráněno odvození architektury systému včetně jeho obranných mechanismů. Dodává, že „[v] *praxi by takto upravené (anonymizované) verze ztratily informační hodnotu, jednalo by se pak pouze o fragmentární souhrn, který by nemohl mít dostatečnou užitečnost pro veřejnou kontrolu*“.

[19] Ve vztahu k variantě částečného poskytnutí informace dle § 12 informačního zákona žalovaný uvádí, že byla zvažována možnost poskytnutí souhrnného seznamu objevených zranitelností, z něhož by byly vynechány technické detaily. Bylo však shledáno, že i výše uvedeným způsobem upravená verze by mohla posloužit kybernetickým útočníkům k tomu, aby získali přehled o obecně zranitelných místech systému a naplánovali jeho napadení. Následně dodává, že „*v případě druhé možnosti – anonymizaci technických částí (zakrytí IP, názvů, běžných zranitelností a ohrožení – CVE), by* (...) *v poskytnutém dokumentu zůstalo dostatečné množství informací umožňující[ch] odvození obranných mechanismů.*“

[20] Žalovaný dospěl k závěru, že „*sdělování detailních informací o systému, který je součástí* [kritické infrastruktury] *státu, je možné považovat za bezpečnostní riziko a tato skutečnost převažuje nad právem na informace*“, přičemž shledal, že byla naplněna výjimka obsažená v § 11 odst. 1 písm. d) informačního zákona. Zároveň uvedl, že právo na informace představuje nástroj k dosažení transparentnosti veřejné správy, avšak není možné jej využívat k získávání technických dat, které mohou v případě poskytnutí ohrozit bezpečnostní zájmy země. Riziko zneužití vyhodnotil v daném případě jako obzvláště vysoké.

[21] Následně žalovaný argumentoval, že neshledává žádný legitimní kontrolní účel, který by byl plněn případným zveřejněním požadovaných informací. Uvádí, že by jen představovalo poskytnutí „přímé výhody“ kybernetickým útočníkům. Odkazuje na publikaci NÚKIB s názvem „*Penetrační testování – úvod do problematiky*“, v níž je penetrační testování označeno za simulaci reálného útoku. Proto danou zprávu vnímá jako „faktický návod“ k útoku na systém kritické infrastruktury.

[22] Závěrem žalovaný dodává, že neměl k dispozici žádný nástroj, který by mu umožnil vyhovět žalobcově žádosti a zároveň zajistit ochranu daných informací. Z toho důvodu nebylo možné postupovat jinak než žádost odmítnout. Jelikož tak žalovaný dané žádosti z části nevyhověl, vydal v souladu s § 15 odst. 1 informačního zákona rozhodnutí o jejím odmítnutí.

IV. Vyjádření žalovaného

[23] Ve svém vyjádření ze dne 4. 2. 2026 setrval žalovaný na závěrech, ke kterým došel v odůvodnění napadeného rozhodnutí. Žalobu shledává nedůvodnou a požaduje její zamítnutí.

V. Posouzení věci Městským soudem v Praze

[24] Městský soud v Praze přezkoumal napadené rozhodnutí, včetně řízení, jež jeho vydání předcházelo, v mezích žalobních bodů, jimiž je vázán, vycházeje přitom ze skutkového a právního stavu, který tu byl v době rozhodnutí správního orgánu (ust. § 75 odst. 1, 2 zákona č. 150/2002 Sb., soudní řád správní – dále jen „*s. ř. s.*“), a o důvodnosti podané žaloby uvážil takto.

[25] Zdejší soud se nejprve zabýval otázkou splnění podmínek přípustnosti žaloby ve smyslu ustanovení § 5 s. ř. s., kde se uvádí: „*Nestanoví-li tento nebo zvláštní zákon jinak, lze se ve správním soudnictví domáhat ochrany práv jen na návrh a po vyčerpání řádných opravných prostředků, připouští-li je zvláštní zákon*.“ Jelikož bylo rozhodnutí o odmítnutí žádosti vydáno ústředním správním úřadem, mohl žalobce napadnout prvostupňové rozhodnutí povinného subjektu pomocí rozkladu. Jak sám žalobce podrobně popsal v rámci rubriky „Přípustnost žaloby“ v podané žalobě, rozhodl se správní žalobou napadnout již prvostupňové rozhodnutí, jelikož se obával dalších obstrukcí ze strany povinného subjektu, proti nimž se již dvakrát bránil žalobou na ochranu proti nečinnosti u zdejšího soudu (usnesení ve věci 17 A 34/2025 a rozsudek ve věci 18 A 75/2025). V této souvislosti žalobce odkazoval na závěry formulované rozšířeným senátem Nejvyššího správního soudu v jeho rozsudku ze dne 24. 10. 2018, č. j. 7 As 192/2017-35. Konkrétně upozorňoval na jeho bod 40, kde je uvedeno: „(...) *žadatel o informace může ve věcech svobodného přístupu k informacím podat žalobu přímo proti rozhodnutí povinného subjektu, kterým povinný subjekt po předchozím zrušovacím rozhodnutí odvolacího orgánu znovu odmítl požadovanou informaci poskytnout*“. Zdejší soud zároveň připomíná i jeho bod 38, kde rozšířený senát uvedl, že „*ochrana ve věcech svobodného přístupu k informacím je specifická a nesmí být v žádném případě formalistická. Proto podá-li žadatel o informaci žalobu proti rozhodnutí povinného subjektu poté, co povinný subjekt opětovně rozhodl způsobem pro žalobce negativním, nesmí správní soud takovouto žalobu odmítnout, ale musí ji věcně projednat, samozřejmě jsou-li dány ostatní podmínky řízení. Je to totiž právě toto rozhodnutí, které*

zasahuje do žalobcovy právní sféry.“ Ve světle výše citovaných závěrů dospěl zdejší soud k tomu, že žaloba je přípustná, a proto pokračoval v jejím věcném projednání, jelikož byly naplněny i ostatní podmínky řízení.

[26] Z obsahu správního spisu soud zjistil, že odmítnutí žalobcovy žádosti napadeným rozhodnutím žalovaného bylo odůvodněno ustanovením § 15 odst. 1 informačního zákona ve spojení s ustanoveními § 11 odst. 1 písm. d) téhož zákona a rovněž ustanovením § 10a kybernetického zákona. Na tomto místě soud poznamenává, že na základě ustanovení § 75 odst. 1 s. ř. s. soud rozhoduje dle právního stavu, jenž tu byl v době rozhodování správního orgánu, tedy v době vydání napadeného rozhodnutí. Jelikož toto bylo vydáno dne 24. 10. 2025, přezkoumává soud dané rozhodnutí na základě právní úpravy účinné k danému dni. Ačkoli tedy došlo mezitím ke zrušení kybernetického zákona č. 181/2014 Sb. a od 1. 11. 2025 nabyl účinnosti zákon č. 264/2025 Sb. (se shodným názvem), nemá tato změna ve vztahu k nyní posuzované věci význam.

[27] Dle ustanovení § 11 odst. 1 písm. d) informačního zákona platí, že omezení poskytnutí požadované informace může povinný subjekt provést v případě, kdy „*její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku nebo připravenosti na krizové situace a jejich řešení*“.

[28] Dle ustanovení § 10a kybernetického zákona platilo: „*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, se podle předpisů upravujících svobodný přístup k informacím neposkytují.*“

[29] V odůvodnění napadeného rozhodnutí žalovaný sám odkazoval na ustanovení § 12 informačního zákona, který mu ukládá povinnost poskytnout požadované informace, a to po vyloučení těch, o kterých tak stanoví zákon. Žalovaný se zabýval i tím, zda neexistuje možnost poskytnout žalobci alespoň částečnou informaci, což popsal na str. 3 a 4 odůvodnění napadeného rozhodnutí. Se samotným důvodem pro odmítnutí poskytnutí informace však soud nesouhlasí, přičemž prozatím není jasné, co vlastně tomuto odmítnutí brání, proto prozatím nepřistoupil k stanovení povinnosti povinnému subjektu informace poskytnout.

[30] Žalovaný nejprve posuzoval (str. 3, poslední odstavec), zda by bylo možné zprávy poskytnout za současného odstranění detailů o objevených zranitelnostech. Zde však žalovaný dospěl k závěru, že i zbylé informace (zde dával za příklad strukturu sítí, typy používaných komponent apod.) by stále postačovaly případným útočníkům k tomu, aby získali přehled o celkovém obrazu systému, a aby odhadli jeho další nedostatky.

[31] Dále se žalovaný zabýval tím, zda by bylo možné daného účelu dosáhnout zakrytím IP adres, názvů serverů a konkrétních CVE (str. 4, první odstavec). Žalovaný tuto možnost anonymizace označuje za nedostatečnou, jelikož by stále umožňovala, aby útočníci odvodili architekturu daného systému a obranných mechanismů. Zároveň uvádí, že by „*takto upravené (anonymizované) verze ztratily*

informační hodnotu, jednalo by se pak pouze o fragmentární souhrn, který by nemohl mít dostatečnou užitečnost pro veřejnou kontrolu“.

[32] Žalovaný zohledňoval i možnost poskytnutí souhrnného seznamu, který by obsahoval objevené zranitelnosti, avšak bez uvedení technických detailů (str. 4, druhý odstavec). Rovněž zde žalovaný usoudil, že by i tato revize stále obsahovala takové informace, které by byli útočníky využitelné k identifikaci zranitelností, objevení slabých míst a připravení kybernetického útoku.

[33] Soud dále shledal, že součástí správního spisu je rovněž „Vyjádření MKB (pozn. soudu – manažera kybernetické bezpečnosti) k požadavku na poskytnutí výsledných zpráv z penetračního testování systémů digitálního stavebního řízení, zpracovaných společnostmi ESET a DCIT (zakázky č. VZ/2024/034/1064 a VZ/2024/034/1074)“. V tomto vyjádření bylo uvedeno, že dle názoru manažera kybernetické bezpečnosti je poskytnutí této informace skrze informační zákon vyloučeno, jelikož požadované zprávy „*obsahují kromě jiného detailní technické popisy nalezených zranitelností, interní strukturu systému, ale i další citlivé informace o stavu bezpečnosti testovaných systémů*“.

[34] Žalobce brojil proti závěru žalovaného v napadeném rozhodnutí, že nelze žalobci poskytnout ani část informací z předmětných zpráv, dle slov žalovaného „*ani po nejintenzivnějším možném redakčním zásahu*“. Soud z obsahu správního spisu zjistil, že se žalobce již v rámci podaného rozkladu ze dne 6. 5. 2025 vymezoval proti postupu žalovaného spočívajícím v odmítnutí jeho žádosti v celém rozsahu. S odkazem na argumentaci žalovaného, kde uváděl, že požadované zprávy „obsahují kromě jiného“ citlivé informace, žalobce namítal, že mělo být postupováno vyčleněním citlivých informací a následným poskytnutím informací zbývajících.

[35] Zároveň soud shledal, že žalobce shodně v podané žalobě i v rámci rozkladu zdůrazňoval časové hledisko, které musí být vždy posouzeno ve vztahu k riziku vyplývajícímu ze zveřejnění daných informací. Žalobce v této souvislosti odkazoval na zranitelnosti, o kterých se veřejnost mohla dočíst v médiích. Současně argumentoval, že s ohledem na opravení daných chyb již nadále nebyl důvod k tomu, aby nebyla poskytnuta alespoň část předmětných zpráv týkající se opravených chyb, o kterých již veřejnost ví. Zároveň podotýkal, že od okamžiku spuštění systému stavebního řízení již byla provedena změna technického řešení - tzv. bypass. Dle názoru žalobce proto není důvod k neposkytnutí informací týkajících se těchto „odstavených“ systémů.

[36] Jak zdejší soud konstatoval například v žalobcem odkazovaném zrušujícím rozsudku ve věci 9 A 161/2019, je povinností žalovaného důsledně vypořádat každou část požadované zprávy, kterou dle jeho názoru není možné poskytnout. V nyní posuzovaném případě soud shledal, že žalovaný sice v rámci odůvodnění napadeného rozhodnutí předložil vysvětlení důvodů, které považuje za převažující nad žalobcovým právem na informace, avšak poskytl vždy jen obecné zhodnocení, namísto toho, aby se dostatečně vyjádřil ke všem částem, které považuje za nezveřejnitelné. Zároveň se podle názoru soudu příliš nekryje obsah možného neposkytnutí informace s tím, co skutečně žalobce žádal.

[37] Nelze souhlasit s žalovaným ve vztahu k jeho argumentaci, že poskytnutí alespoň zbytkových částí zpráv není možné provést, jelikož by se tím „*zničila*

informační hodnota dokumentu“. Soud zde podotýká, že podobně formulované tvrzení nebylo shledáno relevantním ani ve výše uvedeném zrušujícím rozsudku devátého senátu zdejšího soudu (viz bod 78 daného rozsudku). Není totiž na žalovaném, aby posuzoval tuto zbytkovou informační hodnotu, pokud jsou dané informace žadatelem požadovány. Pokud žalovaný odmítne informaci poskytnout, musí konkrétně zdůvodnit, z jakého důvodu jde o „*…informaci, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona…* “ (ust. § 10a kybernetického zákona), a to ve vztahu, co skutečně žalobce žádal a čeho se domáhal ve svých podáních (*„jakou metodou testování probíhalo (např. OWASP TOP 10), a jaký počet zranitelností v jednotlivých stupních závažnosti (kritická, vysoká, střední, nízká) byl zjištěn*“). Zatím není vůbec zřejmé, jak by mohla metoda testování (např. žalobcem zmíněná velmi obecná a rozšířená metoda OWASP TOP 10, která testuje 10 nejkritičtějších bezpečnostních rizik) dosáhnout takové informační důslednosti, že by informace o tom, zda byla tato metoda použita, mohla ohrozit zajišťování kybernetické bezpečnosti; to je závěr naprosto absurdní. Totéž je možné konstatovat o naprosto všech testovacích metodách, přičemž vztah mezi sdělením informace o tom, zda tato metoda byla použita, či nikoliv, k ochraně kybernetické bezpečnosti je nulový. Stejně samotný počet zranitelností v jednotlivých stupních závažnosti podle názoru soudu těžko samo o sobě naplní ohrožení kybernetické bezpečnosti u systému, který je vytvářen na základě zákona a do nějž jsou vkládány údaje touto právní normou vyžadované, a to jak s ohledem na samotné údaje, tak s ohledem na proces jejich vkládání. Žalobce přece nepožadoval konkrétní uvedení těchto zranitelností, ale jejich počet s rozlišením jejich závažnosti. Z odůvodnění napadeného rozhodnutí neplyne, proč by tato informace byla tak zásadní, že by u systému, který má provádět zákon (který sám žádnou utajenou informací být nemůže), měla naplňovat nějaké bezpečnostní riziko.

[38] Je pochopitelné a jistě zdůvodnitelné, proč by konkrétní zjištění zranitelnosti mohlo dát případnému útočníkovi návod, jak systém napadnout. To je legitimní postoj. Není však jasné, proč by takový návod měl dát pouze výčet těchto zranitelností bez vztahu k tomu, co takovou zranitelností bylo, nebo dokonce použitá metoda testování.

[39] Žalovaný se rovněž v napadeném rozhodnutí nevyjádřil ve vztahu k námitce žalobce, kde poukazoval na odpadnutí důvodu k nezveřejnění té části zpráv, která se týká odstavených částí systému. Rovněž neposkytl vyjádření k požadavku na poskytnutí částí pojednávajících o zranitelnostech, které již byly opraveny, a proto dle žalobce jejich zveřejnění nepředstavuje riziko, a to i s ohledem na informace, které se veřejnost dozvěděla z médií. Tyto argumenty žalobce uváděl nejen v rámci podané žaloby, ale již v rámci rozkladových bodů (požadavku na zprávy o výsledku penetračního testování DSŘ se žalobce věnoval na str. 2 rozkladu, který rovněž tvoří obsah správního spisu, a které toto napadené rozhodnutí pomíjí). Výše uvedené námitky však nebyly ze strany žalovaného v napadeném rozhodnutí nijak vypořádány. Zároveň na ně žalovaný nereagoval ani ve svém vyjádření k žalobě, které je stejně jako odůvodnění rozhodnutí pouze obecné a nereaguje na podstatu souzené věci (tedy obsah požadované informace).

[40] Soud výše uvedeným nepopírá význam rizika ohrožení bezpečnosti ani snahu o minimalizaci hrozby kybernetických útoků, ta zde je a v současné době je reálná. Na druhou stranu je však zapotřebí, aby žalovaný vypořádal veškeré námitky, které žalobce v rámci správního řízení uváděl (viz výše), a to zejména u takové informace, která byla veřejností široce diskutována i s ohledem na její výsledek a množství veřejných prostředků, které na ni byly vynaloženy, a která se svou obecností nevztahuje primárně na zjištění možných rizik, ale spíše na efektivitu vynaložených veřejných prostředků na takový systém, který (zřejmě) nebyl schopen plnit své základní funkce. Jak již soud konstatoval výše, není na žalovaném, aby posuzoval „zbytkovou" informační hodnotu těch částí, u nichž zvažoval případné poskytnutí. Žalovaný má pouze přezkoumatelně zdůvodnit, proč nemohl zveřejnit vyčleněné části požadovaných zpráv.

VI. Závěr a rozhodnutí o nákladech řízení

[41] S ohledem na výše popsané došel zdejší soud k závěru, že nebyly naplněny důvody k odmítnutí žalobcovy žádosti o poskytnutí předmětných informací. Soud prozatím přistoupil jen ke zrušení napadeného rozhodnutí z důvodu vady řízení spočívající v jeho nepřezkoumatelnosti způsobené nedostatečným zdůvodněním rozhodnutí a nevypořádáním některých žalobcových námitek vznesených v průběhu správního řízení (ustanovení § 76 odst. 1 písm. a) s. ř. s.). Proto soud vrátil žalovanému věc zpět k dalšímu řízení (ustanovení § 78 odst. 4 s. ř. s.). Nebylo tak zatím postupováno dle § 16 odst. 6 informačního zákona, kdy by soud žalovanému jako povinnému subjektu nařídil informace poskytnout. Žalovaný tak musí znovu posoudit, zda jsou dány důvody k poskytnutí žalobcem požadovaných informací, přičemž je při tomto vázán výše formulovaným právním názorem zdejšího soudu.

[42] Ve věci soud rozhodl rozsudkem bez nařízení jednání, neboť postupoval podle ust. § 76 odst. 1 písm. a) s. ř. s., navíc účastníci proti takovému postupu neměli ve stanovené lhůtě námitek a jednání k projednání žaloby nebylo nutné, když soud neprováděl další dokazování (ust. § 51 odst. 1 s. ř. s.).

[43] Výrok o náhradě nákladů řízení je odůvodněn ust. § 60 odst. 1 s. ř. s., podle kterého má účastník, který měl ve věci úspěch, právo na náhradu nákladů řízení před soudem. Vzhledem k tomu, že ve věci byl úspěšný žalobce, má nárok na tyto náklady řízení. Tyto náklady tvoří zaplacený soudní poplatek ve výši 3 000 Kč, který je žalovaný povinen žalobci zaplatit ve lhůtě 30 dnů od právní moci tohoto rozsudku.

Poučení:

Proti tomuto rozhodnutí lze podat kasační stížnost ve lhůtě dvou (2) 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 dne 7. května 2026

JUDr. Ladislav Hejtmánek, v.r.
předseda senátu