Zpracování DPIA a penetrační testování systémů

Zveřejnění dle § 5 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „InfZ“)

Ministerstvu pro místní rozvoj (dále jen „MMR“) bylo dne 14. 2. 2025 doručeno podání žadatele, z jehož obsahu je zřejmé, že jeho podatel žádá o poskytnutí informace ve smyslu InfZ, zaregistrované podatelnou pod č.j. MMR-14135/2025-31. **Žadatel svým podáním požádal o:**

1. sdělení, kdo je zpracovatelem posouzení vlivu na ochranu osobních údajů (DPIA) u systému na evidenci ubytovatelů a ubytovaných (eTurista),
2. poskytnutí informace, jaký je termín dokončení tohoto DPIA,
3. smlouvu na zpracování předmětného DPIA; v případě, že je již zveřejněna v registru smluv, postačí odkaz na ni; pokud už DPIA byla dokončena, žádám o její poskytnutí, a
4. 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).

Odpověď:

Přípisem MMR ze dne 7. 4. 2025, č. j. MMR-30574/2025-31, byl žadateli zaslán odkaz na smlouvu na zpracování podkladů pro analýzu DPIA zveřejněnou v registru smluv. Dále k prvnímu a druhému bodu žádosti MMR sdělilo, že zpracovatelem posouzení vlivu na ochranu osobních údajů (DPIA) k registru ubytovacích zařízení a ubytovaných osob, označovaného jako eTurista, je odbor cestovního ruchu MMR. Termín dokončení DPIA je závislý na průběhu legislativního procesu a není tedy stanoven fixním datem. Po posouzení zbývajícího obsahu žádosti a v souvislosti s požadavkem pod body 3) a 4) žádosti vydalo dne 25. 4. 2025 rozhodnutí o částečném odmítnutí poskytnutí informace vedené pod č. j. MMR-33456/2025-31.

Proti tomuto rozhodnutí podal žadatel dne 6. 5. 2025 rozklad. Rozhodnutím ministra pro místní rozvoje ze dne 3. 6. 2025, č.j. MMR-40468/2025-31, jímž bylo podle § 152 odst. 5 písm. a) a § 90 odst. 1 písm. b) správního řádu označené rozhodnutí o částečném odmítnutí zrušeno a věc byla vrácena MMR k novému projednání. MMR opakovaně posoudilo požadavek na zpřístupnění požadovaných dokumentů, v němž opakovaně uvedlo, že mu není znám způsob, kterým by bylo současně možné ochránit požadované informace a zároveň je zpřístupnit žadateli. Odmítnutí poskytnutí informací bylo podle názoru MMR jediným možným postupem v dané věci. Poskytnutí informace bylo tedy rozhodnutím ze dne 24. 10. 2025, č.j. MMR-70418/2025-31, odmítnuto, a to podle § 15 odst. 1 InfZ ve spojení s § 11 odst. 1 písm. d) InfZ a § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

Žadatel proti uvedenému rozhodnutí podal správní žalobu k Městskému soudu v Praze, který svým rozsudkem ze dne 7. 5. 2026, č.j. 6 A 154/2025-32 zrušil výše označené rozhodnutí MMR, jímž bylo odmítnuto poskytnutí zpráv z provedeného penetračního testování systémů DSŘ zpracovaných společnostmi ESET a DCIT. Nadepsaný soud věc vrátil MMR k dalšímu řízení s tím, aby znovu posoudilo, zda jsou dány důvody pro (ne)poskytnutí požadovaných informací, a aby své závěry podrobněji odůvodnilo; soud současně vytkl, že předchozí rozhodnutí nebylo dostatečně konkrétní, zejména pokud jde o posouzení možnosti částečného poskytnutí informací podle § 12 InfZ.

MMR v dalším řízení znovu posoudilo žádost nejen jako požadavek na poskytnutí celých výsledných zpráv, ale rovněž z hlediska možnosti poskytnout dílčí, agregované nebo anonymizované informace. Za tím účelem si MMR vyžádalo odborné stanovisko manažera kybernetické bezpečnosti, které je součástí spisu. **MMR došlo k závěru, že požadované informace lze poskytnout pouze částečně, a to z následujících důvodů.**

Na základě odborného stanoviska Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a po meziresortním projednání vláda České republiky určila informační systém DSŘ jako informační systém kritické infrastruktury (položka 534 – Informační systém podporující služby stavebního řízení a územního plánování). Na tento systém se tak vztahuje režim ochrany podle krizového zákona i podle zákona o kybernetické bezpečnosti (dále jen „ZoKB“), zejména

povinnost zajišťovat bezpečnostní opatření a omezení poskytování informací, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti.

Zprávy z penetračního testování obsahují:
- detailní technické popisy nalezených zranitelností, konfigurací a přístupových mechanismů,
- architekturu systému, síťové topologie a rozhraní,
- popisy využitých metod testování a simulací útoků,
- doporučení k nápravě a vyhodnocení zbytkového rizika.

Z povahy těchto údajů je zřejmé, že se jedná o citlivé bezpečnostní informace, jejichž zpřístupnění by mohlo umožnit identifikaci slabin systému a usnadnit přípravu cíleného kybernetického útoku, a jako s takovými je nutné s těmito informacemi zacházet. Požadované zprávy z penetračního testování představují svou povahou ryze technické dokumenty popisující vnitřní nastavení a zabezpečení informační infrastruktury. Nelze je považovat za veřejně dostupné a nelze je tedy zveřejnit. K těmto informacím mají přístup jen ty osoby, které je potřebují pro výkon své činnosti. Pokud by se tyto informace dostaly do nepovolaných rukou, mohly by ohrozit provoz daného systému a výrazně usnadnit případný útok na systém. Jejich zpřístupnění by nepřispělo k prohloubení věcné veřejné kontroly výkonu veřejné správy, nýbrž by mohlo vést k narušení technické integrity a bezpečnosti dotčených systémů, což je v rozporu se smyslem a účelem InfZ.

Za situace, kdy správci informačních systémů kritické infrastruktury současně vystupují jako povinné subjekty podle InfZ, a kdy zároveň dochází k nárůstu kybernetických hrozeb, je nezbytné přistupovat k zajištění kybernetické bezpečnosti se zvýšenou mírou obezřetnosti. Potenciálním útočníkům proto nesmí být zpřístupněny informace, které by mohly ohrozit zabezpečení těchto systémů, a to ani prostřednictvím žádostí o informace. Zpřístupnění takových informací by totiž mohlo být zneužito k cílenému útoku a vést ke vzniku závažných následků. V daném případě je zřejmé, že poskytnutím požadovaných informací by došlo k výraznému zvýšení rizika kybernetického útoku a k ohrožení zajištění kybernetické bezpečnosti.

Podle § 11 odst. 1 písm. d) InfZ povinný subjekt neposkytne informaci, pokud by její poskytnutí významně nebo přímo ohrozilo 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.

Podle § 36 ZoKB se informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, neposkytují, přičemž, jak již bylo uvedeno, toto ustanovení představuje speciální právní důvod (lex specialis) vůči InfZ a týká se všech informací o ochraně, bezpečnostních opatřeních a zranitelnostech prvků KI.

MMR v reakci na rozsudek Městského soudu v Praze č. j. 6 A 154/2025-32 v rámci posouzení žádosti a provedeného testu proporcionality analyzovalo možnost alespoň částečného zpřístupnění požadovaných informací ve smyslu § 12 InfZ:

<u>K metodě testování</u>

DCIT – Test webových aplikací vycházel z metodiky OWASP Web Security Testin Guide (WSTG). Byly též využívány vlastní zkušenosti a postupy zpracovatele. Zvláštní důraz byl věnován na manuální průzkum aplikace podpořený automatizovanými skeny zranitelností.

ESET – Test webových aplikací vycházel z metodiky OWASP Web Security Testin Guide (WSTG). Dále došlo k ověření v rozsahu relevantních kapitol metodiky OWASP Web Security Testing Guide. U penetračního testování infrastruktury nebylo, vzhledem k výrazným limitacím, možné postupovat podle některé z obecně uznávaných metodik pro bezpečnostní testování infrastruktury. Pracovníci ESET proto postupovali dle interní metodiky společnosti ESET, která byla vytvořena specificky pro tento projekt a zohledňovala již zmiňované limitace.

O statistice zranitelností a opravených chybách

Počet zranitelností dle stupně závažnosti ke dni testování (07/2024)

- Kritické: 4 Vyřešeno 4
- Vysoké: 13 Vyřešeno 12
- Střední: 22 Vyřešeno 14
- Nízké: 39 Vyřešeno 23

Z pohledu aktuálního stavu:

- Odstraněná zjištění: převládající část
- Částečně eliminovaná: marginální počet
- Dosud neodstraněná: omezený počet

MMR dále uvádí, že:

- část méně závažných zjištění je zařazena do vývojové pipeline,
- další postup u části zjištění závisí na kapacitách a koordinaci dodavatelů.
- zjištění, která byla odstraněna, již nepředstavují bezpečnostní riziko.

Informace vztahující se k částem systému, které nebyly uvedeny do provozu, byly odstaveny nebo byly nahrazeny jiným technickým řešením, nebo opraveny

MMR sdělilo, že žádná část systému DSŘ nebyla v době testování odstavena z provozu, nedošlo k nahrazení ani omezení provozu z důvodu testování.

Informace o zranitelnostech, které byly podle tvrzení žadatele již popsány ve veřejném prostoru

MMR se zabývalo argumentem, podle něhož se některé z požadovaných informací již objevily ve veřejném prostoru, zejména v médiích (např. článek *Stavební řízení se skandální „dírou“. Cizí dokumenty mohl číst, kdo chtěl - iDNES.cz*), a jejich neposkytnutí tedy postrádá opodstatnění. Na základě opakovaného prověření dostupných mediálních výstupů však MMR nezjistilo, že by v daném případě došlo k úniku konkrétních relevantních informací, které by bylo možné v souladu se InfZ a ZoKB zveřejnit.

Údaje o časovém a personálním rozsahu testování

ESET – test probíhal od 24. 6. 2024 do 4. 7. 2024

DCIT – test probíhal od 1. 7. 2024 do 12. 7. 2024

Informace o personálním rozsahu testování nejsou MMR známy.

O mozaikovém efektu

MMR je při vyřizování žádosti podle InfZ vázáno vymezením požadované informace, jak jej určil žadatel, a poskytuje výhradně informace, které jsou předmětem žádosti.

MMR tedy posoudilo možnost částečného poskytnutí, přičemž na základě technického posouzení manažera kybernetické bezpečnosti dospělo k závěru, že lze uveřejnit:

- agregované statistické údaje,
- metodu testování,

Nelze uveřejnit:

- detailní popisy zranitelností,
- architektura systému,
- konfigurace a integrační vazby,
- testovací postupy a scénáře,
- konkrétní nálezy
- konkrétní bezpečnostní opatření.

Dle technického zdůvodnění existuje riziko mozaikového efektu, kdy mohou být i dílčí nebo zobecněné informace kombinovány s dalšími dostupnými daty a použity k:

- rekonstrukci bezpečnostního profilu systému,
- identifikaci slabých míst,
- prioritizaci cíleného útoku.

MMR proto poskytuje tři zprávy o provedených penetračních testech, na nichž byla provedena redakce (začernění) za účelem omezení rozsahu informací obsažených v původních zprávách z penetračního testování tak, aby bylo minimalizováno riziko jejich zneužití a bylo možné je zveřejnit.

Cílem redakce bylo zejména:

- odstranit přímé technické identifikátory, zejména konkrétní údaje o zranitelnostech, konfiguracích, systémových komponentách a dalších technických aspektech,
- omezit možnost identifikace konkrétní architektury a technologického řešení, včetně vazeb mezi jednotlivými částmi systému,
- eliminovat informace využitelné pro reprodukci testovacích scénářů nebo odvození způsobu napadení,
- snížit riziko nepřímé analýzy bezpečnostního stavu systému, zejména s ohledem na kombinovatelnost jednotlivých informací a tzv. mozaikový efekt.

Začerněny byly informace:

- z kterých by se dala dovodit architektura řešení (označení komponent),
- jsou návodné pro realizaci útoku na aplikace nebo interní infrastrukturu,
- popisují komponenty aplikace a použité technologie,
- popisuje vlastnosti informačního systému,
- přímo popisuje ukázky dotazů a odpovědí pro útok.

Začernění všech nálezů bylo provedeno proto, že:

- jejich zveřejnění by mohlo vést k přímé nebo nepřímé identifikaci slabých míst systému a jeho architektury,
- aktuální stav jejich odstranění není nezávisle ověřen a systém musí být považován za potenciálně zranitelný,
- i historická zjištění mohou být nadále relevantní pro identifikaci nových, variantních chyb, které mohly vzniknout v důsledku nedokonalých oprav nebo regresí, a
- jejich kombinace umožňuje analýzu bezpečnostního profilu systému.

MMR jako povinný subjekt nezpochybňuje právo žadatele na kontrolu hospodaření veřejné správy, včetně kontroly efektivity vynakládání veřejných prostředků. Nicméně dospělo k závěru, že poskytnutí kompletních požadovaných informací by nevedlo k efektivnímu výkonu této kontroly, nýbrž by naopak mohlo představovat bezpečnostní riziko. Nemožnost poskytnutí kompletních požadovaných zpráv nespočívá v jejich formálním utajení, nýbrž v jejich faktickém obsahu. V souladu s judikaturou Nejvyššího správního soudu platí, že ochrana informací o bezpečnostních opatřeních je namístě i tehdy, pokud tyto informace nejsou formálně klasifikovány jako utajované. Rozhodujícím kritériem je totiž reálná možnost jejich zneužití. Vzhledem k tomu, že penetrační zprávy detailně popisují architekturu sdílené infrastruktury (Kubernetes, virtualizace), MMR i nadále zastává názor, že jejich zveřejnění by fakticky poskytlo návod k narušení bezpečnosti dotčených systémů.

V této souvislosti je třeba zdůraznit, že povinností orgánu veřejné moci není prokazovat vznik konkrétní škody ani existenci již probíhajícího útoku. K odmítnutí žádosti postačuje kvalifikovaná úvaha povinného subjektu, že zpřístupněním požadovaných informací by mohlo dojít k ohrožení chráněného zájmu, v daném případě bezpečnosti informačních systémů DSŘ. Jak již bylo uvedeno, zprávy z penetračního testování obsahují popisy konkrétních zranitelností a vektorů útoku na sdílenou infrastrukturu, představují tedy informace, jejichž zneužití je vysoce pravděpodobné, a jejich ochrana proto v rámci testu proporcionality převažuje nad právem na informace.

MMR nadále setrvává na stanovisku, že zveřejnění všech informací obsažených ve výsledných zprávách z penetračního testování systému DSŘ nesleduje legitimní kontrolní účel; naopak by takový postup objektivně vedl k poskytnutí výhody potenciálním útočníkům a ke zvýšení bezpečnostních rizik. MMR současně konstatuje, že z jeho úřední činnosti je mu známo, že informace tohoto typu podléhají přísnému režimu ochrany a standardně se nezpřístupňují.