Kancelář ministryně obrany

Ministerstvo obrany, Tychonova 1, Praha 6 – Hradčany, PSČ 160 01, datová schránka hjyaavk

Praha 7. února 2025
Čj. MO 122168/2025-8694
Sp. zn. SpMO 11860/2025-8694

Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 61/2006 Sb.

Ministerstvo obrany obdrželo dne 26. ledna 2025 Vaši žádost o poskytnutí informací – aktuálních vydání interních aktů řízení Ministerstva obrany, které se týkají platných pokynů upravujících oblast kybernetické a informační bezpečnosti. Mělo by se jednat o dokumenty, které vznikly dle zák. č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, k zajištění opatření kybernetické bezpečnosti (zákon o kybernetické bezpečnosti).

Ministerstvo obrany (dále také jen „ministerstvo“) stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 5 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Ministerstvo obrany disponuje více než 120 dokumenty tohoto typu.

Ustanovení § 10a zákona o kybernetické bezpečnosti stanoví, že *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*.

Důvodová zpráva k zákonu 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony k nově navrhovanému § 10a uvádí:

Navržená úprava vychází ze stávající právní úpravy omezující poskytování informací podle zákona o svobodném přístupu k informacím. Tato úprava 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.

Tato úprava byla dle předkladatele tohoto návrhu zákona velmi omezená již v době přijímání zákona o kybernetické bezpečnosti. V současné době, kdy již bylo určeno 155 významných informačních systémů, spravovaných 58 subjekty, a 48 systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy potenciálních povinných subjektů podle zákona o svobodném přístupu k informacím, a kdy roste počet útoků v kybernetickém prostoru, je zapotřebí přistoupit k opatření i v obecnější rovině zajišťování kybernetické bezpečnosti. Je zapotřebí zdůraznit, že v současnosti účinná výjimka uvedená v § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím nenaplňuje požadavky na ochranu citlivých informací, zejména těch, které se vztahují k přijatým bezpečnostním opatřením podle 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, i v souladu s čl. 1 odst. 6 směrnice (Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.) a recitály č. 2 (Rostoucí rozsah, četnost výskytu a dopad bezpečnostních incidentů představují pro fungování sítí a informačních systémů významnou hrozbu. Uvedené systémy se rovněž mohou stát snadným cílem úmyslných škodlivých akcí za účelem poškození nebo narušení provozu systémů. ...) a č. 8 (Touto směrnicí by neměla být dotčena možnost jednotlivých členských států přijmout nezbytná opatření, aby zajistily ochranu podstatných zájmů své bezpečnosti, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů. ...) směrnice 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. (...)

Podle tohoto návrhu zákona se také neposkytují 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 Listiny základních práv a svobod, 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.

Vzhledem ke specifičnosti oblasti kybernetické bezpečnosti byla výjimka z povinnosti poskytovat informace podle zákona o svobodném přístupu k informacím nově začleněna, obdobně jako je tomu i v některých dalších právních předpisech (srov. např. § 40 zákona o obcích, § 3b zákona o České národní bance, § 27 odst. 2 krizového zákona), přímo do zákona o kybernetické bezpečnosti.

Dle zákonné dikce tak postačuje již samotná možnost ohrožení zajišťování kybernetické bezpečnosti nebo účinnosti opatření. Dokumenty, které vznikly dle zákona o kybernetické bezpečnosti, se rozumí bezpečnostní dokumentace, kterou jsou dle ustanovení § 4 odst. 2 zákona o kybernetické bezpečnosti orgány a osoby uvedené v § 3 písm. c) až f) zákona (povinné osoby), mezi které patří i ministerstvo obrany, povinny vést o bezpečnostních opatřeních, které jsou uvnitř povinné osoby zavedeny a prováděny pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému.

Ministerstvo přistoupilo k posouzení, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti a vzalo do úvahy níže uvedené skutečnosti.

V § 30 odst. 2 písm. e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), je stanoveno, že bezpečnostní

politika a bezpečnostní dokumentace musí být chráněny z pohledu důvěrnosti, integrity a dostupnosti.

Poskytnutí informací o obsahu bezpečnostních opatření, natož jejich zveřejnění, vede automaticky ke snížení účinnosti takového opatření, což má zároveň zpravidla za následek, a tedy může způsobit, ohrožení zajišťování kybernetické bezpečnosti. Důvodem pro snížení účinnosti takového opatření jeho zveřejněním nebo i jen zpřístupněním neoprávněné osobě je, že z bezpečnostní dokumentace nebo bezpečnostní politiky může neoprávněná osoba zjistit zranitelnosti nebo slabá místa v bezpečnosti informací a kybernetické bezpečnosti, a to i v dokumentech týkajících se poučování zaměstnanců. Tato slabá místa a zranitelnosti mohou být následně zneužity při plánování vektoru útoku na organizaci, čímž se zvyšuje šance, že kybernetický útok bude úspěšný. Uvedené nabývá na významu obzvláště za situace, kdy musí být poskytnuté informace dle ustanovení § 5 odst. 3 zákona č. 106/1999 Sb. následně zveřejněny způsobem umožňujícím dálkový přístup.

Přestože pohnutky žadatele pro podání informace jsou při způsobu vyřizování jeho žádosti irelevantní, byl při posouzení, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti, vzat v úvahu fakt, že žadatel sám zamýšlí poskytnuté informace přeložit a vědomě šířit dál v mezinárodním akademickém a vědeckém prostředí specializujícím se na informační bezpečnost, kde lze očekávat vyšší koncentraci osob schopných zjistit zranitelnosti nebo slabá místa v bezpečnosti informací a kybernetické bezpečnosti, a to i v dokumentech týkajících se poučování zaměstnanců.

Po zvážení všech výše uvedených skutečností nezbývá než požadované informace neposkytnout.