

ZÁKON

ze dne 2021,

kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

Změna zákona o Vojenském zpravodajství

Čl. I

V zákoně č. 289/2005 Sb., o Vojenském zpravodajství, ve znění zákona č. 274/2008 Sb., zákona č. 254/2012 Sb., zákona č. 273/2012 Sb., zákona č. 64/2014 Sb., zákona č. 250/2014 Sb., zákona č. 47/2016 Sb., zákona č. 35/2018 Sb. a zákona č. 205/2019 Sb., se za část třetí vkládá nová část čtvrtá, která včetně nadpisu a poznámek pod čarou č. 19 až 22 zní:

„ČÁST ČTVRTÁ

ČINNOSTI VOJENSKÉHO ZPRAVODAJSTVÍ PŘI ZAJIŠŤOVÁNÍ OBRANY ČESKÉ REPUBLIKY

§ 16a

Činnosti Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru

(1) Vojenské zpravodajství za podmínek stanovených tímto zákonem provádí

- a) cílenou detekci kybernetických útoků a hrozeb majících původ v zahraničí¹²⁾ a směřujících proti důležitým zájmům státu, jejichž zajišťování je předmětem obrany České republiky podle zákona o zajišťování obrany České republiky¹⁹⁾ (dále jen „detekce“),
- b) identifikaci a vyhodnocování detekovaných kybernetických útoků a hrozeb a jejich dopadů (dále jen „vyhodnocování“) a
- c) opatření k odvracení detekovaných kybernetických útoků a hrozeb.

(2) Detekce je Vojenským zpravodajstvím prováděna na základě jím stanovených ukazatelů kybernetických útoků a hrozeb umožňujících odhalit v kybernetickém prostoru definované jevy, které v daném čase byly vyhodnoceny jako skutečnosti ohrožující důležité zájmy státu v kybernetickém prostoru.

(3) Ukazatele kybernetických útoků a hrozeb jsou Vojenským zpravodajstvím stanovovány na základě

- a) dat a informací, které Vojenské zpravodajství získává při plnění svých úkolů jako jednotné ozbrojené zpravodajské služby České republiky,
- b) dat a informací předaných ostatními zpravodajskými službami, Národním úřadem pro kybernetickou a informační bezpečnost a dalšími státními orgány, nebo
- c) dalších skutečností způsobilých ohrozit plnění funkce státu v oblasti zajišťování jeho obrany, které jsou mu předány.

§ 16b

Spolupráce Vojenského zpravodajství při provádění činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru

(1) Při provádění činností a opatření vykonávaných v souvislosti se zajišťováním obrany státu v kybernetickém prostoru spolupracuje Vojenské zpravodajství s ostatními zpravodajskými službami a s dalšími státními orgány, ozbrojenými silami České republiky, bezpečnostními sbory a právníckými a fyzickými osobami, pokud působí v oblasti zajišťování kybernetické bezpečnosti nebo obrany státu.

(2) Při zajišťování detekce Vojenské zpravodajství spolupracuje s právníckými nebo fyzickými osobami zajišťujícími veřejnou komunikační síť nebo poskytujícími veřejně dostupnou službu elektronických komunikací, a to na základě písemné dohody o spolupráci. Dohodou o spolupráci nelze sjednat předávání metadat ve větším rozsahu, než je upraveno v § 16d odst. 2.

(3) Dohoda o spolupráci uzavřená podle odstavce 2 musí obsahovat

- a) technické a organizační podmínky nezbytné pro realizaci detekce,
- b) způsob předávání metadat o zachyceném útoku nebo hrozbě a
- c) způsob určení výše efektivně vynaložených nákladů.

§ 16c

Součinnost při detekci

Pokud Vojenské zpravodajství nemá s právníckou nebo podnikající fyzickou osobou zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací uzavřenu dohodu o spolupráci podle § 16b odst. 2 a hrozilo by nebezpečí z prodlení, je oprávněno si vyžádat od této osoby po nezbytně nutnou dobu součinnost při cíleném vyhledávání konkrétního kybernetického útoku nebo hrozby pomocí ukazatelů v rozsahu bezpečnostních opatření, která tato osoba již provádí.

§ 16d

Nástroje detekce a podmínky jejich provozování

(1) Vojenské zpravodajství může využívat vlastní nástroje detekce, které jsou umístěny pouze pro účely detekce na určených bodech veřejných komunikačních sítí, pokud to vyžaduje důležitý zájem obrany státu a

- a) nelze ani s vynaložením potřebného úsilí dosáhnout uzavření ani změny dohody o spolupráci pro zajišťování detekce podle § 16b odst. 2, nebo
- b) zajišťování detekce na základě dohody o spolupráci uzavřené podle § 16b odst. 2 není účinné.

(2) Nástroj detekce zaznamenává metadata

- a) popisující informace a souvislosti nezbytné pro přenos dat, jejich strukturu a čas o zachyceném provozu veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací, a to pouze v rozsahu souvisejícím s detekovaným kybernetickým útokem nebo hrozbou na základě stanovených ukazatelů; součástí není obsah přenášených dat,
- b) provozu nástroje detekce a

c) o manipulaci s konfigurací nástroje detekce pro potřeby auditu činností vykonávaných Vojenským zpravodajstvím.

(3) Vojenské zpravodajství nesmí využívat nástroje detekce podle odstavce 1 pro provádění odposlechů nebo pro záznam zpráv podle zákona o elektronických komunikacích nebo k aktivnímu zásahu podle § 16f odst. 3.

(4) Vojenské zpravodajství provádí detekci výlučně způsobem, který zaručuje, že

- a) je zachována důvěrnost komunikací fyzických a právnických osob při poskytování veřejně dostupné služby elektronických komunikací, integrita veřejných komunikačních sítí a dostupnost veřejných komunikačních sítí a služeb elektronických komunikací a
- b) není zasahováno nebo ovlivňováno plnění povinností právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací vůči uživatelům sítě, včetně kvality poskytovaných služeb, jinak, než v rozsahu odpovídajícím veřejnému zájmu na zajišťování obrany státu.

§ 16e

Zajištění podmínek detekce

(1) Ministerstvo obrany požaduje pro účely podle § 16d odst. 1 od právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, aby zřídila a zabezpečila v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce.

(2) Základní charakteristiky veřejných komunikačních sítí využitelných pro umístění nástrojů detekce z hlediska zajištění důležitých zájmů státu stanoví vláda v ústředním plánu obrany státu²⁰⁾.

(3) K plnění povinnosti podle odstavce 1 vydá Ministerstvo obrany na základě návrhu Vojenského zpravodajství vypracovaného jako opatření k zajištění závěrů jím plněných povinností stanovených v § 16a odst. 1 a 2 rozhodnutí, jímž právnické nebo podnikající fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací uloží povinnost zřídit a zabezpečit rozhraní pro připojení nástrojů detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování těchto nástrojů.

(4) Rozhodnutí podle odstavce 3 musí vedle náležitostí stanovených správním řádem obsahovat také

- a) určení doby, po kterou má být nástroj detekce v určeném bodě provozován, a
- b) lhůtu, ve které je právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna v určených bodech jí zajišťované veřejné komunikační sítě zřídit rozhraní pro připojení nástroje detekce.

(5) Doba podle odstavce 4 písm. a) nesmí být delší než 12 měsíců; Ministerstvo obrany ji může na návrh Vojenského zpravodajství prodloužit, a to nejvýše o 6 měsíců.

(6) Rozklad proti rozhodnutí nemá odkladný účinek.

(7) Před vydáním rozhodnutí podle odstavce 3 je Vojenské zpravodajství povinno posoudit, zda připojení nástroje detekce samo o sobě není bezpečnostním rizikem, popřípadě zda je možné důsledky takového bezpečnostního rizika přijmout jako akceptovatelné vzhledem k účelu připojení konkrétního nástroje detekce. Dokument obsahující závěry takového posouzení je podkladem pro vydání rozhodnutí podle odstavce 3.

(8) Před vydáním rozhodnutí o prodloužení lhůty podle odstavce 5 je Ministerstvo obrany povinno vždy posoudit, zda jsou splněny podmínky podle § 16d. Rozhodnutí o prodloužení lhůty obsahuje určení doby, po kterou má být nástroj detekce v určeném bodě dále provozován.

§ 16f

Opatření k odvrácení detekovaných kybernetických útoků a hrozeb

(1) Vojenské zpravodajství na základě výsledku vyhodnocování přijme opatření k odvrácení detekovaných kybernetických útoků a hrozeb podle odstavce 2 nebo 3.

(2) V případě, že identifikuje konkrétní kybernetický útok nebo hrozbu, pro jejichž odvrácení nejsou naplněny podmínky pro provedení aktivního zásahu podle § 16g, předá neprodleně zjištěné informace k provedení dalších opatření příslušným státním orgánům. Zjištěné informace v nezbytně nutném rozsahu může předat také provozovateli národního CERT²¹⁾, pokud vyhodnotí, že je to pro účely zajištění kybernetické bezpečnosti státu účelné. V případech hodných zvláštního zřetele může předat informace v nezbytně nutném rozsahu také další osobě, která s jejich využitím může provést opatření směřující proti kybernetickému útoku či hrozbě.

(3) Hrozí-li nebezpečí z prodlení, provede Vojenské zpravodajství za podmínek stanovených v § 16g aktivní zásah k neprodlenému odvrácení detekovaného kybernetického útoku či hrozby.

§ 16g

Oprávnění provést aktivní zásah v kybernetickém prostoru

(1) Vojenské zpravodajství je oprávněno provést aktivní zásah výlučně v případě, že

- a) skutečnosti jím zjištěné v kybernetickém prostoru svědčí o existenci ohrožení důležitých zájmů státu ve značném rozsahu,
- b) kybernetický útok nebo hrozba směřující proti důležitým zájmům státu trvají nebo bezprostředně hrozí a
- c) kybernetický útok nebo hrozbu směřující proti důležitým zájmům státu nelze odvrátit v součinnosti s ozbrojenými silami České republiky a aktivní zásah byl vyhodnocen jako jediný možný účinný způsob jejich odvrácení.

(2) K provedení aktivního zásahu je Vojenské zpravodajství oprávněno pouze po předchozím souhlasu ministra obrany.

(3) O zahájení aktivního zásahu Vojenské zpravodajství bezodkladně informuje vládu, Národní úřad pro kybernetickou a informační bezpečnost a ostatní zpravodajské služby.

(4) Vojenské zpravodajství o provedení aktivního zásahu bezodkladně po jeho provedení informuje ministra obrany a jeho prostřednictvím

- a) vládu,
- b) náčelníka Generálního štábu Armády České republiky,
- c) ředitele Národního úřadu pro kybernetickou a informační bezpečnost a
- d) ostatní zpravodajské služby.

(5) Pro obsah předávané informace podle odstavce 4 se využije § 16h odst. 2 obdobně.

(6) Jestliže nedojde k ohrožení důležitého zájmu státu, může být v nutném rozsahu informován i provozovatel národního CERT²¹⁾.

(7) Vojenské zpravodajství poskytne v souvislosti s jím prováděnými činnostmi a opatřeními, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, v této oblasti působnosti součinnost Národnímu úřadu pro kybernetickou a informační bezpečnost nebo Policii České republiky, pokud o to v individuálních případech výlučně pro účely jimi zajišťované bezpečnosti České republiky v kybernetickém prostoru požádají; tím není dotčena součinnost výkonu veškerých činností Vojenského zpravodajství prováděných podle této části vůči ozbrojeným silám České republiky při zajišťování obrany státu.

§ 16h

Záznamy o předání dat a informací nebo aktivním zásahu a jejich uchovávání

(1) Pokud Vojenské zpravodajství v rámci zajištění součinnosti pro provádění činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, předává data a informace, které jsou výstupem jím prováděné detekce a vyhodnocování, zpracuje o tomto předání záznam obsahující charakteristiku předávaných dat a informací v rozsahu skutečností uvedených v odstavci 2 písm. a) až c) a e), účel předání dat a informací a dále údaje o době předání dat a informací a identifikační údaje adresáta jejich předání v rozsahu:

- a) název adresáta,
- b) adresa, na kterou byly data a informace předány,
- c) časový údaj předání dat a informací s přesností na sekundy,
- d) časový údaj o potvrzení převzetí dat a informací s přesností na sekundy.

(2) Vojenské zpravodajství je povinno o každém provedeném aktivním zásahu provést záznam, a to minimálně v rozsahu:

- a) charakteristika identifikovaného útoku nebo hrozby směřující proti důležitým zájmům státu,
- b) závěry posouzení útoku nebo hrozby směřující proti důležitým zájmům státu,
- c) závěry posouzení přípustnosti provedení aktivního zásahu,
- d) údaje o zdroji útoku nebo hrozby směřující proti důležitým zájmům státu,
- e) časový údaj o provedení opatření směřujících k zastavení nebo odvrácení útoku anebo odstranění hrozby s přesností na sekundy,
- f) způsob provedení zásahu a popis využitých organizačních a technických opatření,
- g) další skutečnosti charakterizující provedení aktivního zásahu.

(3) Záznamy podle odstavců 1 a 2 Vojenské zpravodajství uchovává po dobu 10 let od data jejich zpracování.

§ 16i

Zprávy o činnostech Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru

(1) Vojenské zpravodajství předkládá prezidentu republiky a vládě prostřednictvím ministra obrany jednou ročně podrobnou zprávu o činnostech a opatřeních Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, a vyhodnocení jejich účinnosti.

(2) Vojenské zpravodajství předkládá ministru obrany neprodleně po ukončení kalendářního pololetí písemnou zprávu o stavu jím plněných úkolů, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, za toto období.

§16j

Nepřípustnost použití dat a informací k jiným účelům

Data a informace získané Vojenským zpravodajstvím při provádění detekce nesmí být použity pro jiné účely než zabezpečování činností, jimiž se podílí na zajišťování obrany státu, pokud tento zákon nestanoví jinak.

16k

Inspektor pro kybernetickou obranu

(1) Vláda České republiky jmenuje a odvolává na návrh ministra obrany inspektora pro kybernetickou obranu; návrh je vládě České republiky překládán po jeho projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti.

(2) Inspektor pro kybernetickou obranu je jmenován na dobu 5 let.

(3) Inspektor pro kybernetickou obranu je vojákem z povolání nebo zaměstnancem zařazeným ve Vojenském zpravodajství a je podřízen přímo ministrovi obrany, nestanoví-li tento zákon jinak.

(4) Ve věcech služebního nebo pracovního poměru inspektora pro kybernetickou obranu činí právní úkony jménem České republiky ministr obrany.

(5) Inspektor pro kybernetickou obranu je při plnění úkolů podle § 16l odst. 1 písm. a) a b) nezávislý a je vázán pouze právním řádem České republiky; je povinen svou funkci vykonávat nestranně, v mezích svého oprávnění a zdržet se při jejím výkonu všeho, co by mohlo ohrozit důvěru v jeho nestrannost a profesionalitu.

(6) Vojenské zpravodajství je povinno zajistit, aby byl inspektor pro kybernetickou obranu náležitě, včas a v potřebném rozsahu zapojen do veškerých záležitostí souvisejících s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru, zejména mu poskytuje veškeré potřebné informace o provádění detekce a vyhodnocování. Vojenské zpravodajství zároveň zabezpečuje materiální a personální podmínky výkonu funkce inspektora pro kybernetickou obranu.

(7) Inspektor pro kybernetickou obranu předává ministru obrany vždy neprodleně po ukončení kalendářního pololetí zprávu o jím zjištěných nedostatcích v oblasti zajišťování ochrany dat a informací zpracovávaných Vojenským zpravodajstvím při výkonu činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru; zpráva obsahuje rovněž návrhy opatření na zkvalitnění ochrany soukromí a osobních údajů. V případě zjištění závažného nedostatku zprávu předává inspektor pro kybernetickou obranu ministru obrany bezodkladně po jeho zjištění, a to včetně návrhů na jeho odstranění a přijetí preventivních opatření.

§ 16l

Úkoly inspektora pro kybernetickou obranu

(1) Inspektor pro kybernetickou obranu vykonává tyto úkoly:

- a) prověřuje správnost postupů Vojenského zpravodajství při činnostech, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, pokud se týkají zabezpečení ochrany dat a informací,

- b) ověřuje účinnost opatření přijatých Vojenským zpravodajstvím za účelem zajišťování ochrany dat a informací zpracovávaných při činnostech, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, podílí se na jejich zavádění do činnosti Vojenského zpravodajství a navrhuje jejich případnou aktualizaci,
- c) při činnostech Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, poskytuje na vyžádání poradenskou podporu příslušníkům Vojenského zpravodajství v oblasti ochrany dat a informací,
- d) za účelem zajištění účinnosti opatření přijímaných k ochraně práv spolupracuje se subjekty, u nichž byly umístěny nástroje detekce podle § 16e.

(2) Právnícké nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací se mohou obracet na inspektora pro kybernetickou obranu ve všech záležitostech souvisejících se zajištěním jejich práv, pokud jsou nebo by mohly být ohroženy činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru.

(3) Inspektor pro kybernetickou obranu podnět prošetří a na základě zjištěných skutečností vypracuje zprávu, se kterou seznámí Poslaneckou sněmovnu a osobu, která podnět podala.

§ 16m

Kontrola činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, a prověřování souvisejících opatření

(1) Provádí-li vláda, Poslanecká sněmovna nebo orgán nezávislé kontroly²²⁾ kontrolu činností a opatření Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, je Vojenské zpravodajství povinno kontrolujícímu předložit zejména

- a) záznamy podle § 16h a
- b) další zprávy, které jsou nezbytné pro zjištění skutečného stavu v rozsahu nezbytném pro dosažení účelu kontroly.

(2) Kontrolující podle odstavce 1 jsou oprávněni požádat o

- a) přístup k auditním záznamům provozu nástroje detekce,
- b) přístup ke spisové dokumentaci vedené ve věci rozhodování o umístění nástroje detekce, nebo
- c) poskytnutí dalších dat a informací souvisejících s předmětem kontroly.

(3) Kontrolující je při provádění kontroly povinen šetřit práva a oprávněné zájmy Vojenského zpravodajství, stejně jako třetích osob, kterým byly v souvislosti s prováděním činností Vojenského zpravodajství podle této části uloženy povinnosti.

(4) Kontrolní řád se na kontrolu činnosti Vojenského zpravodajství podle této části nepoužije.

(5) Na prověřování opatření přijímaných Vojenským zpravodajstvím v zájmu zabezpečování činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, Ministerstvem obrany se použije ustanovení § 41 zákona o zajišťování obrany České republiky obdobně.

§ 16n

Náhrada škody nebo nemajetkové újmy

(1) Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu.

(2) Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru.

(3) Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která vyvolala útok nebo hrozbu.

(4) Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.

¹⁹⁾ § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

²⁰⁾ § 2 písm. a) nařízení vlády č. 139/2017 Sb., o plánování obrany státu.

²¹⁾ § 17 zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

²²⁾ § 12 zákona č. 153/1994 Sb., ve znění pozdějších předpisů.“.

Dosavadní části čtvrtá až šestá se označují jako části pátá až sedmá.

ČÁST DRUHÁ

Změna zákona o zpravodajských službách České republiky

Čl. II

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění zákona č. 118/1995 Sb., zákona č. 53/2004 Sb., zákona č. 290/2005 Sb., zákona č. 530/2005 Sb., zákona č. 80/2006 Sb., zákona č. 342/2006 Sb., zákona č. 250/2008 Sb., zákona č. 274/2008 Sb., zákona č. 218/2009 Sb., zákona č. 227/2009 Sb., zákona č. 357/2011 Sb., zákona č. 254/2012 Sb., zákona č. 170/2013 Sb., zákona č. 186/2013 Sb., zákona č. 64/2014 Sb., zákona č. 204/2015 Sb., zákona č. 219/2015 Sb., zákona č. 51/2016 Sb., zákona č. 251/2017 Sb., zákona č. 325/2017 Sb., zákona č. 35/2018 Sb., zákona č. 205/2019 Sb. a zákona č. 227/2019 Sb., se mění takto:

1. V § 2 se dosavadní text označuje jako odstavec 1 a doplňuje se odstavcem 2, který včetně poznámek pod čarou č. 10 a 11 zní:

„(2) Vojenské zpravodajství se v rozsahu a způsobem stanoveným zákonem o Vojenském zpravodajství¹⁰⁾ podílí¹¹⁾ na zajišťování obrany České republiky v kybernetickém prostoru.

¹⁰⁾ Část čtvrtá zákona č. 289/2005 Sb., ve znění zákona č. .../2021 Sb.

¹¹⁾ Čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky.“.

2. V § 12 odst. 1 se na konci textu věty první doplňují slova „ ; kontrole kontrolujícími podléhá rovněž činnost Vojenského zpravodajství, kterou se podílí na zajišťování obrany státu v kybernetickém prostoru podle zákona o Vojenském zpravodajství¹⁰⁾“.
3. V § 12e odst. 1 se věta druhá zrušuje.
4. V § 12e odst. 2 se na konci písmene b) čárka nahrazuje slovem „a“.
5. V § 12e odst. 2 se písmeno c) zrušuje.
Dosavadní písmeno d) se označuje jako písmeno c).

ČÁST TŘETÍ

Změna zákona o elektronických komunikacích

Čl. III

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb., zákona č. 303/2013 Sb., zákona č. 181/2014 Sb., zákona č. 234/2014 Sb., zákona č. 250/2014 Sb., zákona č. 258/2014 Sb., zákona č. 318/2015 Sb., zákona č. 378/2015 Sb., zákona č. 222/2016 Sb., zákona č. 298/2016 Sb., zákona č. 183/2017 Sb., zákona č. 194/2017 Sb., zákona č. 225/2017 Sb., zákona č. 252/2017 Sb., zákona č. 287/2018 Sb., zákona č. 277/2019 Sb., zákona č. 311/2019 Sb. a zákona č. 403/2020 Sb., se mění takto:

1. Za § 98 se vkládá nový § 98a, který včetně poznámek pod čarou č. 70 až 72 zní:

„§ 98a

(1) Právnícká nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na základě rozhodnutí vydaného Ministerstvem obrany podle zákona o Vojenském zpravodajství⁷⁰⁾ zřídit a zabezpečit v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce umožňujícího provádět cílenou detekci jevů nasvědčujících existenci kybernetického útoku nebo hrozby a jejich identifikaci podle zákona o Vojenském zpravodajství⁷¹⁾.

(2) Právnícká nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytne neprodleně na vyžádání součinnost při cíleném vyhledávání kybernetického útoku nebo hrozby pomocí

ukazatelů podle zákona o Vojenském zpravodajství⁷²⁾ v rozsahu a prostřednictvím bezpečnostních opatření, které tato osoba již provádí.

(3) Osoba uvedená v odstavci 1 není bez souhlasu Vojenského zpravodajství oprávněna zasáhnout do jím připojeného nástroje detekce nebo jakkoliv omezit jeho funkčnost; to neplatí, pokud provedení zásahu do nástroje detekce nebo omezení jeho funkčnosti je nutné vzhledem k tomu, že v souvislosti s jeho připojením a provozováním je vyvolán stav ohrožující samotný provoz veřejné komunikační sítě, poskytování veřejně dostupné služby elektronických komunikací nebo ohrožující zdraví anebo životy fyzických osob, hrozí-li nebezpečí z prodlení.

(4) Osoba uvedená v odstavci 1 je povinna umožnit Vojenskému zpravodajství na požádání přístup k nástroji detekce umístěnému na jí zajišťované veřejné komunikační síti, přičemž Vojenské zpravodajství musí postupovat tak, aby jeho činností nebyly porušovány podmínky výkonu povinností této osobě uložené zákonem.

(5) Za plnění povinností podle odstavce 1 náleží právnické nebo podnikající fyzické osobě od Vojenského zpravodajství úhrada efektivně vynaložených nákladů. Způsob určení výše efektivně vynaložených nákladů, postup jejich uplatnění a způsob jejich úhrady stanoví prováděcí právní předpis.

(6) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavců 1 a 2, jsou povinny zachovávat mlčenlivost o všech skutečnostech souvisejících s prováděním detekce a s připojením a užíváním nástroje detekce. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první.

(7) Povinnost zachovávat mlčenlivost podle odstavce 6 se nevztahuje na podávání informací kontrolujícím, kteří provádějí kontrolu činností Vojenského zpravodajství podle části čtvrté zákona o Vojenském zpravodajství.

⁷⁰⁾ § 16e zákona č. 289/2005 Sb., ve znění zákona č. .../2021 Sb.

⁷¹⁾ § 16a odst. 2 zákona č. 289/2005 Sb., ve znění zákona č. .../2021 Sb.

⁷²⁾ § 16c zákona č. 289/2005 Sb., ve znění zákona č. .../2021 Sb.“.

2. V § 118 se za odstavce 22 vkládá nový odstavec 23, který zní:

„(23) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující veřejnou komunikační síť nebo veřejně dostupnou službu elektronických komunikací dopustí přestupku tím, že

- a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce podle rozhodnutí vydaného Ministerstvem obrany,
- b) v rozporu s § 98a odst. 2 neposkytne součinnost,
- c) neumožní Vojenskému zpravodajství přístup k nástroji detekce,
- d) neoprávněně zasáhne do nástroje detekce nebo omezí jeho funkčnost, nebo
- e) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 6.“.

Dosavadní odstavec 23 se označuje jako odstavec 24.

3. V § 118 odst. 24 písm. a) se slova „nebo odstavce 14 písm. ae)“ nahrazují slovy „, , odstavce 14 písm. ae) nebo odstavce 23 písm. e)“.

4. V § 118 odst. 24 písm. b) se slova „nebo odstavce 15“ nahrazují slovy „ , odstavce 15 nebo odstavce 23 písm. b), c) anebo d)“.
 5. V § 118 odst. 24 písm. c) se slova „nebo 22“ nahrazují slovy „ , 22 nebo 23 písm. a) “.
 6. V § 119 se za odstavec 6 vkládá nový odstavec 7, který zní:
„(7) Fyzická osoba podílející se na plnění povinností právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo veřejně dostupnou službu elektronických komunikací se dopustí přestupku tím, že poruší povinnost zachovávat mlčenlivost podle § 98a odst. 6.“.
- Dosavadní odstavec 7 se označuje jako odstavec 8.
7. V § 119 odst. 8 větě první se číslo „6“ nahrazuje číslem „7“.
 8. V § 150 se doplňuje odstavec 7, který zní:
„(7) Ministerstvo obrany ve spolupráci s Úřadem vydá vyhlášku k provedení § 98a odst. 5.“.

ČÁST ČTVRTÁ

Změna zákona o vojácích z povolání

Čl. IV

Zákon č. 221/1999 Sb., o vojácích z povolání, ve znění zákona č. 155/2000 Sb., zákona č. 129/2002 Sb., zákona č. 254/2002 Sb., zákona č. 362/2003 Sb., zákona č. 546/2005 Sb., zákona č. 189/2006 Sb., zákona č. 261/2007 Sb., zákona č. 305/2008 Sb., zákona č. 306/2008 Sb., zákona č. 479/2008 Sb., zákona č. 272/2009 Sb., zákona č. 326/2009 Sb., zákona č. 147/2010 Sb., zákona č. 375/2011 Sb., zákona č. 470/2011 Sb., zákona č. 122/2012 Sb., zákona č. 332/2014 Sb., zákona č. 204/2015 Sb., zákona č. 377/2015 Sb., zákona č. 47/2016 Sb., zákona č. 183/2017 Sb., zákona č. 263/2017 Sb., zákona č. 181/2018 Sb., zákona č. 32/2019 Sb. a zákona č. 285/2020 Sb., se mění takto:

1. V § 3 se za odstavec 1 vkládá nový odstavec 2, který zní:
„(2) Vyžaduje-li to důležitý zájem služby, může být občan ve výjimečných případech povolán do služebního poměru, i když nesplňuje kvalifikační předpoklady nebo podmínky zdravotní způsobilosti stanovené pro služební místo ve Vojenském zpravodajství, na které má být služebně zařazen.“.

Dosavadní odstavec 2 se označuje jako odstavec 3.

2. V § 6 se na konci odstavce 3 doplňuje věta „Vyžaduje-li to důležitý zájem služby, může být příslušník Vojenského zpravodajství ve výjimečných případech služebně zařazen na služební místo, i když nesplňuje požadovanou kvalifikaci.“.
3. V § 6a se na konci odstavce 1 doplňuje věta „Ustanovení o rozhodné době se nevztahují na příslušníky Vojenského zpravodajství.“.
4. V § 48 se na konci odstavce 1 tečka nahrazuje čárkou a doplňuje se písmeno k), které zní:
„k) podrobit se na pokyn služebního orgánu vyšetření na polygrafu, když je příslušníkem Vojenského zpravodajství.“.

ČÁST PÁTÁ

Účinnost

Čl. V

Tento zákon nabývá účinnosti dnem 1. července 2021.