Pozměňovací návrh poslance Zbyňka Stanjury k vládnímu návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony

(sněmovní tisk 931)

1. V čl. I "změna zákona o Vojenském zpravodajství" v bodě 2 se doplňuje text § 16a odst. 2 zákona o Vojenském zpravodajství a celé znění § 16a odst. 2 je následující:

"(2) Vojenské zpravodajství může při zajišťování kybernetické obrany využívat technické prostředky kybernetické obrany, kterými jsou věcné technické prostředky **s výlučně pasivními prvky, které umožňují pouze monitorování a analýzu provozu sítí a služeb elektronických komunikací.** ~~vedoucí k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany České republiky;~~ Vojenské zpravodajství využívá při zajišťování kybernetické obrany společně s technickými prostředky kybernetické obrany k dosažení shodného účelu také související postupy a opatření."

2. V čl. I "změna zákona o Vojenském zpravodajství" v bodě 2 se doplňuje text § 16b a celé znění § 16b je následující:

"§ 16b

Předpoklady umístění a použití technických prostředků kybernetické obrany

Umístění technických prostředků kybernetické obrany podle §16a může být provedeno výlučně na základě jeho schválení vládou, která rovněž schválí podmínky jejich používání k zajištění kybernetické obrany **a obsah smluvního ujednání mezi Vojenským zpravodajstvím a povinným subjektem**. Návrh na umístění technických prostředků kybernetické obrany, jehož součástí je také návrh podmínek jejich používání, předkládá vládě ředitel Vojenského zpravodajství prostřednictvím ministra obrany."

3. V čl. I "změna zákona o Vojenském zpravodajství" v bodě 2 se na konci textu § 16c doplňuje věta, která zní:

„Vojenské zpravodajství v žádosti uvede technické podmínky plnění povinnosti právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací a poskytne právnické nebo podnikající fyzické osobě zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací další potřebnou součinnost.“.

4. V čl. III "změna zákona o elektronických komunikacích" v bodě 2 se v § 98a na konec odstavce 1 doplňuje text „s výlučně pasivními prvky“ a za něj se vkládají nové odstavce 2, 3 a 5, takže celý § 98a ve znění pozměňovacího návrhu má tuto podobu:

„§ 98a

(1) Právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací

nebo poskytující službu elektronických komunikací je povinna, je-li o to požádána za účelem plnění úkolů kybernetické obrany Vojenským zpravodajstvím na základě zákona o Vojenském zpravodajství, zřídit a zabezpečit ve vhodných bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany **s výlučně pasivními prvky**.

(2) Osoba uvedená v odstavci 1 je oprávněna odpojit nebo odmítnout připojit rozhraní nebo technický prostředek kybernetické obrany za mimořádných okolností, je-li to nezbytné pro zajištění bezpečnosti a integrity její sítě elektronických komunikací nebo služeb elektronických komunikací, ochranu před škodlivou interferencí nebo narušením funkčnosti sítě. Je-li to možné, osoba uvedená v odstavci 1 současně nabídne alternativní řešení pro splnění povinnosti podle odstavce 1.

(3) Rozsah povinnosti dle odstavce 1 bude vymezen smlouvou, o které je povinná osoba dle odst. 1 povinna s Vojenským zpravodajstvím jednat a návrh smlouvy předložit k posouzení Úřadu. Vláda na základě závazného stanoviska Úřadu návrh smlouvy dle předchozí věty přezkoumá a uloží povinné osobě dle odst. 1 povinnost smlouvu s Vojenským zpravodajstvím uzavřít. Součástí rozhodnutí dle předchozí věty bude úplné znění smlouvy.

(~~2~~**4**) 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 a způsob jejich úhrady stanoví prováděcí právní předpis.

(5) Právnická nebo podnikající fyzická osoba podle odstavce 1 neodpovídá za porušení své právní povinnosti, způsobené v souvislosti s plněním povinností vyplývajících z odstavce 1 a smlouvy uzavřené dle odstavce 3 nebo v souvislosti s připojením či použitím technických prostředků kybernetické obrany[1].

(~~3~~**6**) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce 1, jsou povinny zachovávat mlčenlivost o připojení technických prostředků kybernetické obrany podle odstavce 1 a s tím souvisejících skutečnostech. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první.“.

Dosavadní odstavce 2 a 3 se označují jako odstavce 4 a 6.

5. V čl. III "změna zákona o elektronických komunikacích" v bodě 3 se do § 118 odst. 22 písm. a) doplňuje text „s výlučně pasivními prvky“, takže celý § 118 odst. 22 ve znění pozměňovacího návrhu má tuto podobu:

„(22) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací dopustí správního deliktu tím, že

a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech své sítě rozhraní
pro připojení technických prostředků kybernetické obrany **s výlučně pasivními prvky** na žádost Vojenského zpravodajství, nebo

b) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 3.“.

[1] § 16a zákona č. 289/2005 Sb., o Vojenském zpravodajství

Odůvodnění pozměňovacího návrhu:

K bodu 1 (čl. I, § 16a odst. 2)

Dle vládního návrhu bylo možné do stávajících veřejných sítí elektronických komunikací umísťovat i technické prostředky, které aktivně zasahují do provozu v sítích, např. generují falešný provoz či provádějí další kybernetický útok nebo protiútok, případně jakkoli jinak narušují provoz. Je třeba vzít v úvahu, že tyto sítě jsou provozovány soukromými podnikateli a slouží k poskytování veřejných komunikačních služeb. Konstrukce a kapacity těchto sítí tedy nejsou budovány pro účely aktivní obrany státu a jejich využití pro tento účel může vést k přetížení či jiným nepředvídaným stavům sítě.

Jakákoli diagnostika poruchy s instalovanými jinými než pasivními prvky by byla ztížena – aby tomu tak nebylo, museli by zaměstnanci Vojenského zpravodajství být členem servisní skupiny operátora. Vojenské zpravodajství by instalací jiných než pasivních prvků de facto převzalo správu páteřní infrastruktury operátora, neboť jakákoli modifikace provozu je de facto zásahem do fungování a řízení sítě. Mimo to mají operátoři nastaveny vlastní mechanismy ochrany sítí proti kybernetickým útokům, které mohou být nasazením aktivních prvků Vojenským zpravodajstvím aktivovány – tím by pak bylo působení aktivních prvků rušeno nebo modifikováno způsobem, který nelze předvídat.

Uvedené skutečnosti mohou vést k omezení fungování sítě či jejímu výpadku, což by mělo zásadní negativní dopady mj. na dostupnost čísel tísňového volání a fungování záchranného systému. Z těchto důvodů se navrhuje upravit zákonem pravomoc Vojenského zpravodajství tak, aby do sítí mohlo umísťovat výlučně technické prostředky kybernetické obrany s pasivními prvky, jimiž lze provoz sítí pouze monitorovat a analyzovat. To rovněž odpovídá dosavadní praxi u policejních odposlechů a přitom umožňuje získat Vojenskému zpravodajství dostatek informací k plánování a realizaci aktivní kybernetické obrany jinými, vhodnějšími prostředky.

K bodu 2 a 3 (čl. I, § 16b a 16c)

Novela obsahuje ohledně rozsahu povinností operátorů relativně obecnou formulaci, která nedává vodítko a nepopisuje proces, jak budou určeny funkce a technické parametry rozhraní, které jsou operátoři povinni zřídit, ani konkrétní další technické podmínky součinnosti ze strany operátorů.

Vojenskému zpravodajství se proto ukládá povinnost předat jako součást žádosti o poskytnutí součinnosti operátorům i technické podmínky plnění povinnosti, které požaduje. To umožní operátorům mimo jiné posoudit možné dopady na zajištění bezpečnosti a integrity jejich sítí.

K bodu 4 (čl. III, § 98a odst. 1, 2, 3 a 5)

<u>Možnost odmítnout připojit nebo odpojit rozhraní nebo technický prostředek kybernetické obrany za mimořádných okolností</u>

Novela předpokládá, že prostřednictvím rozhraní zřízeného operátorem bude Vojenské zpravodajství do sítě elektronických komunikací připojovat technické prostředky kybernetické obrany - tedy vlastní zařízení, která nejsou nikde blíže specifikována a u nichž

vládní návrh nevylučuje ani aktivní působení na síť. To má – kromě pochybností o souladu tohoto záměru s principy ústavního pořádku, které však nejsou předmětem tohoto pozměňovacího návrhu – velmi zásadní technické a právní implikace. Důsledkem použití těchto prostředků, které operátor nemá pod svou kontrolou, může být nejen monitorování provozu, ale též omezení funkčnosti sítě, její chybná funkce nebo výpadek. Realizace povinnosti operátora zřídit rozhraní a připojit technické prostředky kybernetické obrany se tak může dostat do konfliktu s jinými významnými povinnostmi operátora, jejichž plnění je v zájmu osob soukromého i veřejného práva (zajištění bezpečnosti a integrity sítě operátora, ochrana telekomunikačního tajemství).

Operátor prostřednictvím sítě poskytuje řadu služeb: mimo jiné tísňová volání, cloudové služby či zálohování dat pro podnikatele, zaměstnanecké telekomunikační programy, platební služby či technické nástroje k jejich provádění (např. autorizační SMS, datové spojení pro platební terminály) i telekomunikační služby pro nepodnikatele. Na těchto službách často závisí nejen ekonomický prospěch, ale i včasná záchrana zdraví a životů osob. Novela tuto skutečnost opomíjí, a proto je pozměňovacím návrhem doplněna.

Ve výjimečných případech, kdy by zřízení rozhraní a připojení technických prostředků kybernetické obrany mohlo narušit bezpečnost a integritu sítě, by operátor byl oprávněn požadavek Vojenského zpravodajství odmítnout a navrhnout alternativní řešení, případně rozhraní či technický prostředek (dočasně) odpojit nebo odmítnout připojit.

Institut smlouvy, upravující podmínky nasazení technických prostředků kybernetické obrany

Z hlediska transparentnosti a legitimity vztahů mezi oprávněným a povinným subjektem je nezbytné, aby o konkrétních podmínkách použití technických prostředků Vojenské zpravodajství uzavíralo smlouvy s dotčenými operátory, jejichž sítě se toto opatření dotkne. Toto řešení je praktické už kvůli zcela obecné zákonné formulaci, která nedává žádné vodítko, jaká detailní opatření jsou nezbytná, aby nasazení prostředků bylo funkční; přitom je nutné zohlednit i technická specifika konkrétních sítí. Protože navržené znění zákona s uzavíráním zmíněné smlouvy nepočítá, je tento institut doplněn pozměňovacím návrhem.

Pozměňovací návrh svěřuje pravomoc posoudit návrh smlouvy Českému telekomunikačnímu úřadu. To umožňuje navázat na kompetence, které úřad má dle zákona o elektronických komunikacích, zejména to umožňuje zohlednit v návrhu smlouvy i zákonné požadavky na bezpečnost a integritu sítí, což jsou cíle požadované zákonem č. 127/2005 Sb., nad jejichž dodržováním bdí úřad jakožto regulátor. Doplněné ustanovení dává tedy jasný režim tomu, jak bude povinnost k uzavření smlouvy operátorům ukládána.

Omezení odpovědnosti poskytovatele služeb elektronických komunikací

Novela předpokládá, že prostřednictvím rozhraní zřízeného operátorem bude Vojenské zpravodajství do sítě elektronických komunikací připojovat technické prostředky kybernetické obrany - tedy vlastní zařízení, která nejsou nikde blíže specifikována a u nichž vládní návrh nevylučuje ani aktivní působení na síť. Důsledkem použití těchto prostředků, které operátor nemá pod svou kontrolou, může tedy být nejen monitorování provozu, ale též omezení funkčnosti sítě, její chybná funkce nebo výpadek.

Operátor ovšem prostřednictvím sítě poskytuje řadu služeb: mimo jiné tísňová volání, cloudové služby či zálohování dat pro podnikatele, zaměstnanecké telekomunikační

programy, platební služby či technické nástroje k jejich provádění (např. autorizační SMS, datové spojení pro platební terminály) i telekomunikační služby pro nepodnikatele. Na těchto službách často závisí nejen ekonomický prospěch, ale i včasná záchrana zdraví a životů osob. Protože operátor technické prostředky kybernetické obrany neovládá, nemůže být odpovědný za důsledky, které souvisí s jejich připojením a použitím v síti. Novela však tento princip opomíjí, a proto je pozměňovacím návrhem doplněn.

Výluka z odpovědnosti přitom musí dopadat obecně na porušení právní povinnosti operátora, vyvolané použitím technických prostředků kybernetické obrany: tedy nejen porušení povinnosti, kterou stanovuje zákon, ale též smluvních závazků vůči odběratelům či zákazníkům operátora.

K bodu 5 (čl. III, § 118 odst. 22)

Legislativně-technická úprava v souladu s bodem I pozměňovacího návrhu (viz výše).