Návrh zákona Spolkového ministerstva vnitra

Návrh zákona o posílení kybernetické bezpečnosti[1]

Dne ...

Německý spolkový sněm (Bundestag) přijal se souhlasem německé Spolkové rady (Bundesrat) tento zákon:

[…]

Článek 4

Změny zákona o ochraně osobních údajů a soukromí v telekomunikacích a digitálních službách

Zákon o telekomunikacích, digitálních službách a ochraně osobních údajů ze dne 23. června 2021 (Spolk. věst. I s. 1982; 2022 I s. 1045), naposledy pozměněný článkem 3 zákona ze dne 10. března 2026 (Spolk. věst. 2026 I č. 64), se mění takto:

1. za § 19 odst. 4 se vkládají nové odstavce 5 a 6, které znějí takto:

(1) „Pokud se poskytovatel digitálních služeb dozví o poruše, která vznikla v souvislosti s využíváním jedné z jeho služeb uživatelem, je povinen o tom neprodleně informovat uživatele, pokud je mu tento znám. Pokud je to technicky možné a ekonomicky přiměřené, musí poskytovatel v rámci své odpovědnosti za digitální služby nabízené v rámci podnikatelské činnosti upozornit uživatele na přiměřené, účinné a dostupné technické prostředky, pomocí nichž může poruchu rozpoznat a odstranit. Pokud byla porucha poskytovateli nahlášena Spolkovým úřadem pro bezpečnost informačních technologií (BSI), je povinen předat uživateli veškeré informace uvedené v hlášení o poruše, které umožňují poruchu rozpoznat a odstranit. Poskytovatel smí přesměrovat části datového provozu směřujícího k využívané službě, z níž porucha pochází, a od ní, pokud je to nezbytné k tomu, aby mohl uživatele o poruše informovat.

(2) Je-li poskytovatel digitálních služeb informován Spolkovým úřadem pro bezpečnost informačních technologií (BSI) o konkrétních hrozbách pro bezpečnost informačních technologií, které v souvislosti s využíváním jedné z jeho služeb uživatelem vznikají nebo se jí týkají, je povinen o tom neprodleně informovat uživatele, pokud je mu znám. Poskytovatel přitom musí uživateli předat zejména všechny informace obsažené ve sdělení Spolkového úřadu pro bezpečnost informačních technologií (BSI) podle věty 1, pomocí nichž lze tato rizika rozpoznat a předejít jim. Pokud se poskytovatel digitálních služeb dozví o rizicích pro bezpečnost informačních technologií, která vyplývají z využívání jedné z jeho služeb uživatelem nebo se jich týkají, může o tom uživatele informovat. Pokud je to technicky možné a ekonomicky přiměřené, může uživatele upozornit na přiměřené, účinné a dostupné technické prostředky, pomocí nichž může tato rizika rozpoznat a jim předcházet.“

[…]

[1] Článek 4 tohoto zákona oznámený v souladu se směrnicí Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

Odůvodnění

B. Zvláštní část

K článku 4 (Změny zákona o ochraně osobních údajů a soukromí v telekomunikacích a digitálních službách)

K bodu 1

Nově zavedené odstavce 5 a 6 ukládají poskytovatelům digitálních služeb povinnost informovat své uživatele o poruchách (odstavec 5) nebo konkrétních rizicích (odstavec 6), která vyplývají z některé z jejich služeb, a předávat svým uživatelům informace BSI o konkrétních rizicích, která se týkají zákazníků poskytovatelů, pokud jsou tyto známy a je možné o nich informovat.

Povinnosti uvedené v odstavcích 5 a 6 v zásadě odpovídají těm, které již pro poskytovatele telekomunikačních služeb existují v § 169 odst. 5 a 6 zákona o telekomunikacích (TKG). Dosavadní povinnost poskytovatelů telekomunikačních služeb podle § 169 odst. 5 a 6 TKG vykazuje mezery při řešení příslušných nebezpečí, jelikož jsou pravidelně zasaženy i systémy, jejichž provozovatelé nespadají pod TKG. Spolkový úřad pro bezpečnost informací (BSI) však o nich již denně zpracovává mnoho zjištění týkajících se zranitelných nebo napadených systémů (poskytovatelé hostingu, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, provozovatelé sítí pro doručování obsahu, poskytovatelé spravovaných služeb, poskytovatelé spravovaných bezpečnostních služeb). Tyto informace jsou sice v současné době předávány poskytovatelům, ale poskytovatelé služeb je velmi často z důvodu absence zákonné povinnosti nepředávají dotčeným uživatelům. Stávajícímu nebezpečí tak nelze pravidelně účinně čelit.

Odstavce 5 a 6 se vztahují pouze na takové poruchy nebo nebezpečí, která vyplývají z využívání služby uživatelem. Jedná se o případy, kdy uživatel využívá např. hostingovou službu pro provoz webové stránky nebo e-mailové služby a webová stránka nebo e-mailová služba, za kterou odpovídá, je napadena a zneužita k šíření škodlivých programů nebo phishingových e-mailů. Jedná se tedy o poruchy a nebezpečí, které se týkají uživatele v rámci jeho využívání služby. Možnými příklady relevantních poruch jsou napadený e-mailový účet, přes který jsou rozesílány spamové e-maily; napadený server, který je zneužíván k DDoS útokům, nebo napadená webová stránka, přes kterou jsou šířeny škodlivé programy.

Tato povinnost slouží k tomu, aby se předešlo škodám způsobeným zranitelnými nebo již napadenými službami. Takové škody mohou vzniknout jak samotnému uživateli, tak i ostatním uživatelům internetu, pokud jsou napadeni prostřednictvím dotčených služeb (např. škodlivými programy, phishingem nebo DDoS útoky). Kromě toho jsou poskytovatelé digitálních služeb povinni informovat ty uživatele, jejichž využívané služby jsou příčinou poruchy nebo pro něž existuje nebezpečí – pokud je to známo – a předat těmto uživatelům informace, které jim zaslal Spolkový úřad pro bezpečnost informací (BSI).