Osnutek zakona Zveznega ministrstva za notranje zadeve

Osnutek zakona za krepitev kibernetske varnosti[1]

z dne …

Nemški zvezni parlament (Bundestag) je s soglasjem nemškega zveznega sveta (Bundesrat) sprejel naslednji zakon:

[...]

Člen 4

Spremembe zakona o varstvu podatkov in zasebnosti na področju telekomunikacij in digitalnih storitev

Zakon o varstvu podatkov na področju telekomunikacij in digitalnih storitev z dne 23. junija 2021 (Zvezni uradni list I, str. 1982; 2022, str. 1045), kakor je bil nazadnje spremenjen s členom 3 zakona z dne 10. marca 2026 (Zvezni uradni list, 2026, št. 64), se spremeni:

1. za odstavkom 4 oddelka 19 se dodata naslednja odstavka 5 in 6:

   (1) „Če ponudnik digitalnih storitev med uporabo storitve s strani uporabnika ugotovi motnjo, ki izvira iz ene od njegovih storitev, mora o tem nemudoma obvestiti uporabnika, če je identiteta uporabnika znana. Če je to tehnično izvedljivo in ekonomsko razumno, mora ponudnik v okviru svoje odgovornosti za komercialno zagotovljene digitalne storitve uporabnika obvestiti o ustreznih, učinkovitih in dostopnih tehničnih sredstvih, s katerimi lahko zazna in odpravi motnje. Če je ponudnika o motnji obvestil Zvezni urad za informacijsko varnost (BSI), mora ta uporabniku posredovati vse podatke iz obvestila o motnji, ki so potrebni za odkrivanje in odpravo motnje. Ponudnik lahko preusmeri del prometa podatkov, ki poteka v smeri do in iz storitve, ki jo uporablja uporabnik in pri kateri je prišlo do motnje, če je to potrebno za obvestitev uporabnika o tej motnji.

   (2) Če Zvezni urad za informacijsko varnost (BSI) obvesti ponudnika digitalnih storitev o posebnih grožnjah za varnost informacijske tehnologije, ki izhajajo iz ene od njegovih storitev ali vplivajo na uporabnikovo uporabo, mora o tem nemudoma obvestiti uporabnika, če je njegova identiteta znana. Pri tem mora ponudnik uporabniku zlasti posredovati vse informacije iz obvestila Zveznega urada za informacijsko varnost (BSI) v skladu s prvim stavkom, ki omogočajo prepoznavanje in preprečevanje groženj. Če ponudnik digitalnih storitev ugotovi, da obstajajo grožnje za varnost informacijske tehnologije, ki izhajajo iz uporabe ene od njegovih storitev s strani uporabnika ali pa to uporabo vplivajo, lahko o tem obvesti uporabnika. Kadar je to tehnično mogoče in ekonomsko upravičeno, lahko ponudnik uporabniku svetuje glede ustreznih, učinkovitih in dostopnih tehničnih sredstev, s katerimi lahko prepozna in prepreči te grožnje.“.

[...]

---

[1] Člen 4 tega zakona je priglašen v skladu z Direktivo (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe (UL L 241, 17.9.2015, str. 1).

Obrazložitev

B. Posebni del

Opomba k členu 4 (spremembe zakona o varstvu podatkov in varstvu zasebnosti na področju telekomunikacij in digitalnih storitev)

Opomba k točki 1

Z novo uvedenima odstavkoma 5 in 6 morajo ponudniki digitalnih storitev svoje uporabnike obvestiti o motnjah (odstavek 5) ali specifičnih grožnjah (odstavek 6), ki izhajajo iz ene od njihovih storitev, ter posredovati informacije Zveznega urada za informacijsko varnost (BSI) o specifičnih grožnjah, ki vplivajo na stranke ponudnikov, njihovim uporabnikom, če so te informacije znane in je obveščanje mogoče.

Obveznosti iz odstavkov 5 in 6 se v bistvu ujemajo z že obstoječimi obveznostmi za ponudnike telekomunikacijskih storitev iz odstavkov 5 in 6 oddelka 169 zakona o telekomunikacijah. Obstoječe obveznosti ponudnikov telekomunikacijskih storitev v skladu z odstavkoma 5 in 6 člena 169 zakona o telekomunikacijah puščajo vrzeli pri obravnavanju ustreznih groženj, saj so redno prizadeti sistemi, katerih upravljavci niso podvrženi zakona o telekomunikacijah. Vendar Zvezni urad za informacijsko varnost (BSI) dnevno obdeluje številne ugotovitve o ranljivih ali ogroženih sistemih (ponudniki storitev gostovanja, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, operaterji omrežja za zagotavljanje vsebin, upravljani ponudniki storitev, upravljani ponudniki varnostnih storitev). Čeprav se te ugotovitve trenutno posredujejo ponudnikom, jih ponudniki storitev zaradi neobstoja pravne obveznosti zelo pogosto ne posredujejo prizadetim uporabnikom. Zato obstoječe grožnje ni mogoče redno in učinkovito obravnavati.

Odstavka 5 in 6 zajemata le tiste motnje ali grožnje, ki izhajajo iz storitve med uporabo te storitve s strani uporabnika. To se nanaša na primere, ko uporabnik na primer uporablja storitev gostovanja za upravljanje spletnega mesta ali storitve elektronske pošte, spletno mesto ali storitev elektronske pošte, za katero je odgovoren, pa je ogrožena in zlorabljena za distribucijo zlonamerne programske opreme ali lažnih elektronskih sporočil. Gre torej za motnje in grožnje, ki vplivajo na uporabnika, ko ta uporablja storitev. Med možne primere takšnih motenj spadajo: ogrožen e-poštni račun, ki se uporablja za pošiljanje neželene pošte; ogrožen strežnik, ki se uporablja za DDoS-napade; ali ogrožena spletna stran, ki se uporablja za razširjanje zlonamerne programske opreme.

Namen te obveznosti je preprečiti škodo, ki jo povzročajo ranljive ali že ogrožene storitve. Takšna škoda lahko prizadene tako samega uporabnika kot tudi druge internetne uporabnike, če so ti napadeni prek prizadetih storitev (npr. z zlonamerno programsko opremo, lažnim predstavljanjem ali DDoS-napadi). Poleg tega morajo ponudniki digitalnih storitev obvestiti tiste uporabnike, katerih uporaba storitev povzroča motnje ali za katere obstaja nevarnost – če je to znano –, ter tem uporabnikom posredovati vse informacije, ki jih posreduje zvezni urad za informacijsko varnost (BSI).