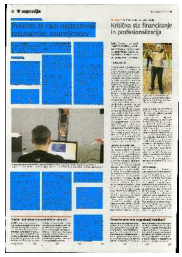
Dnevnik

Država: Slovenija

Stran: 4

Površina: 556 cm^2



25.02.2019
Ponedeljek

1 / 2

PRAVOSODJE / ZAKONODAJA

Policisti bi radi nadzorovali računalnike osumljencev

Na pravosodnem ministrstvu bodo ponovno prisluhnili željam policije po preiskovanju računalnikov osumljencev na daljavo. Nekateri argumenti notranjega ministrstva so utemeljeni, drugi pa zavajajoči.

Peter Lovšin

Čeprav je aktualni okleščeni predlog novele zakona o kazenskem postopku (ZKP) v državnozborski proceduri, se bodo na pravosodnem ministrstvu kmalu začeli ukvarjati že z naslednjo novelo, ki bo potrebna zaradi evropskega javnega tožilstva, ki naj bi zaživelo do konca leta 2020. Na mizi bo ponovno tudi pomembna zakonska podlaga, po kateri bi policija s podtaknjeno programsko opremo ali kako drugače na daljavo nadzorovala (raznovrstne) računalniške sisteme osumljencev.

Že ko je pravosodno ministrstvo vodil **Senko Pličanič**, so potekali resni pogovori, da v tedanji noveli ZKP pristane tudi člen, ki bi opredeljeval, pod kakšnimi pogoji lahko policija na podlagi odredbe preiskovalnega sodnika pri osumljencu namesti »trojanca« – programsko opremo, s katero bi policija lahko dostopala do komunikacije pri viru. Na koncu je bila v skrajšanem postopku v parlamentu sprejeta le pusta novela, ki je zgolj prenesla evropske direktive, Pličaničev naslednik **Goran Klemenčič** pa nameščanju skrite programske opreme ni bil naklonjen. Pravosodno ministrstvo pod vodstvom **Andreje Katič** se je z notranjim ministrstvom in policijo o tej temi zdaj ponovno pripravljeno pogovarjati, predvsem zaradi težav, ki jih imajo policisti pri preiskovanju hujših kaznivih dejanj.

Organizirani kriminal in zavajajoča srečna naključja

Za utemeljevanje potreb so se na ministrstvu za notranje zadeve (MNZ) zatekli k različnim težavam preiskovalcev. Najprepričljivejši so zagotovo povzetki dogovarjanj članov kriminalnih združb, ki se dogovarjajo o nadaljnjih pogovorih prek programa skype ali sorodnih komunikacijskih poti, ki omogočajo šifrirano komunikacijo. Tudi sicer je že dlje časa javna skrivnost, da si člani organiziranih kriminalnih skupin v veliki meri pomagajo s šifrirano komunikacijo, kar lahko policija le nemočno opazuje.

Bistveno manj pa je MNZ prepričljiv z argumenti, da je ta ukrep potreben tudi za splošno varnost v državi. »Takšen primer je bila (teroristična) grožnja z eksplozivnim telesom na nedoločeni železniški postaji. Neznani storilec je iz temačnega spleta poslal elektronsko sporočilo vodstvu Slovenskih železnic, v katerem je zahteval plačilo določene vsote na anonimen račun Bitcoin. V sporočilu je bilo navedeno še, da bo eksplozivno telo, če se plačilo ne izvede, v nekaj dneh eksplodiralo, če plačajo, pa bo sporočena točna lokacija, kje se eksplozivno telo nahaja. Po srečnem naključju do eksplozije ni prišlo,« so zapisali na MNZ, po našem preverjanju pa se je izkazalo, da gre za pretiravanje, če ne celo zavajanje. Ko smo pri policiji preverili, kakšno srečno naključje je preprečilo eksplozijo, smo izvedeli, da bombe sploh ni bilo in da je šlo torej za klasičen lažni alarm oziroma »blef« pošiljatelja.

Težavno nadzorovanje zlorab

Kako zagotoviti učinkovit pregon kriminala, ki bo tudi sorazmeren in v skladu z ustavno zajamčenimi pravicami, hkrati pa bo možnost zlorab orodij preiskovalcev minimalna, je vprašanje, na katero ni lahkih odgovorov.

Dr. **Kaja Prislan** s fakultete za varnostne vede poudarja, da so ustrezni pravni temelji nujen predpogoj za preprečevanje zlorab, obenem pa pri uvajanju novih tehnoloških rešitev izpostavlja tudi problematiko kolateralne škode: »Primera, ki ponazarjata možne kršitve človekovih pravic in kolateralno škodo, sta na primer uporaba vohunskih programov v sklopu prikritih preiskovalnih ukrepov, kjer so izkušnje iz Nemčije pokazale, da so zlorabe težko nadzorljive, in lovilec številk IMSI (tega ureja že aktualna novela ZKP, op. p.), kjer se z njegovo uporabo posega tudi v zasebnost tretjih oseb, ki niso predmet preiskave.«

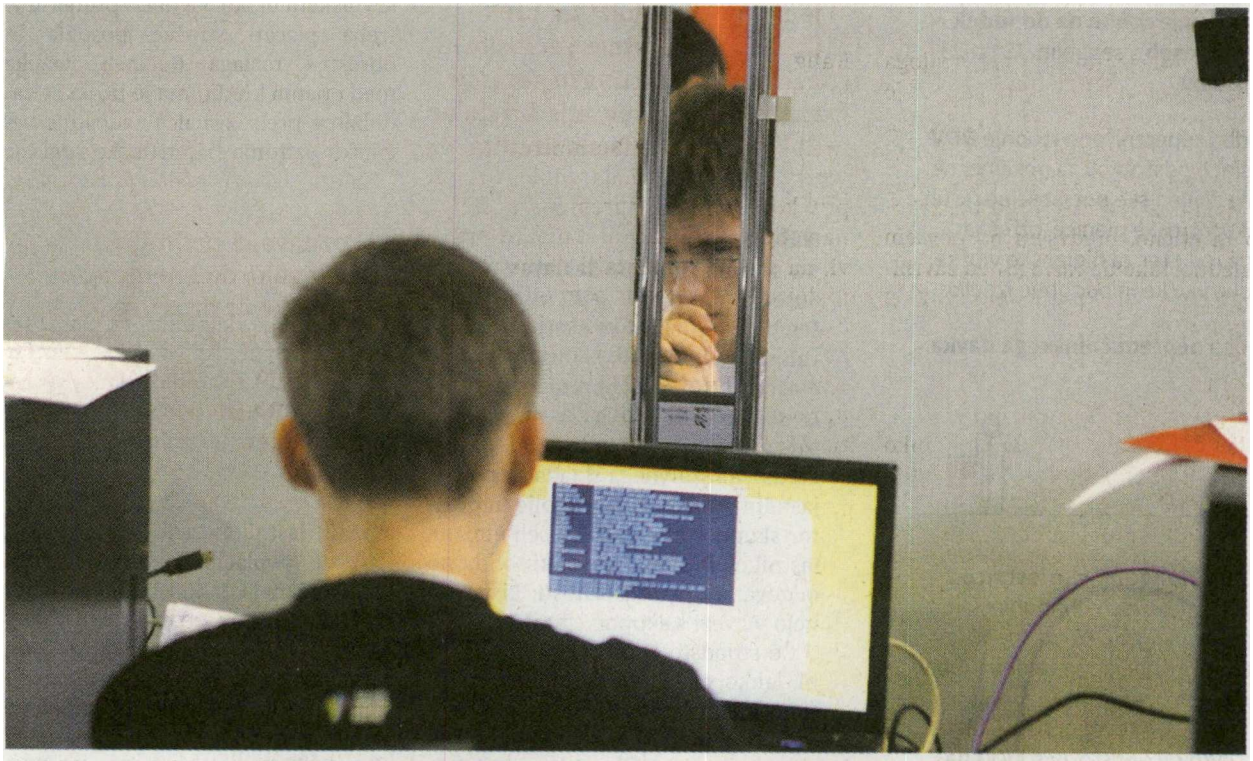
Nekatere države EU so podobne rešitve, kot jih želi MNZ, sicer že sprejele. MNZ poleg Nemčije navaja še pet držav, v Sloveniji pa bo verjetno najprej potrebna razprava, ali glede na varnostno stanje v našem okolju nove ukrepe potrebujemo, in če da, katere. Dr. Prislan ocenjuje, da glede na pravno ureditev drugih evropskih držav Slovenija ni v posebnem zaostanku, zagotovo pa ni v koraku s časom glede razvoja kriminalitete. ×

Že dlje časa je javna skrivnost da si člani organiziranih kriminalnih skupin v veliki meri pomagajo s šifrirano komunikacijo, kar lahko policija le nemočno opazuje.

Kako zagotoviti učinkovit pregon kriminala, ki bo tudi sorazmeren in v skladu z ustavno zajamčenimi pravicami, hkrati pa bo možnost zlorab orodij preiskovalcev minimalna, je vprašanje, na katero ni lahkih odgovorov.

Nadzor nad vsemi računalniškimi sistemi

Na MNZ so se o potrebah za novo orodje ponovno razpisali že v decembrskem dopisu pravosodnemu ministrstvu. Dokument, ki smo ga pridobili v uredništvu in pod katerim je podpisana državna sekretarka Melita Šinkovec, razkriva, da MNZ rešitev ne vidi več le pri prestrezanju podatkov pri viru elektronskih komunikacij, saj ta ne omogoča dostopa do komunikacije na temačnem spletu. MNZ si zato želi, da bi ZKP pod določenimi pogoji dovoljeval nadzor nad vsem vrstami računalniških sistemov. Trenutno zakon o kazenskem postopku dovoljuje le nadzor nad računalniškimi sistemi bank ali drugih pravnih oseb, ki opravljajo finančno ali drugo gospodarsko dejavnost.



Na mizi pravosodnega ministrstva bo ponovno pomembna zakonska podlaga, po kateri bi policija s podtaknjeno programsko opremo ali kako drugače na daljavo nadzorovala računalniške sisteme osumljenih. Bojan Velikonja DOKUMENTACIJA DNEVNIKA