Nacionalni inštitut
za **javno zdravje**

URAD DIREKTORJA
Trubarjeva cesta 2
1000 Ljubljana
Slovenija
t +386 1 2441 400
www.nijz.si
info@nijz.si
ID DDV: SI 44724535
TRR: 011006000043188

Številka: 382-30/2024-1 (083)
Ljubljana, dne: 14. 6. 2024

Združenje zdravstvenih zavodov Slovenije
Riharjeva ulica 38, 1000 Ljubljana
e-mail: gp.zdruzenje@zdrzz.si

Strokovno združenje zasebnih zdravnikov in zobozdravnikov Slovenije
Dunajska 162
1000 Ljubljana
e-mail: info@zdravniki-zobozdravniki.net

Zadeva: Nadgradnja varnostnih protokolov TLS za dostop do eZdravja

Spoštovani,

uporaba informacijske tehnologije v zdravstvu prinaša številne prednosti, npr. omogoča hitrejšo in učinkovitejšo obravnavo pacientov ter drugih uporabnikov zdravstvenih storitev. Vendar ob tem ne smemo spregledati varnostnih tveganj, ki v mednarodnem okolju dobivajo vse večje razsežnosti. Tarče hekerskih napadov so pogosto prav zdravstvenih informacijski sistemi, delno zato, ker predstavljajo vstopno točko v državno kritično infrastrukturo, delno zato, ker so zdravstveni podatki iskano blago na podatkovnem črnem trgu.

Izjemen pomen zagotavljanja ustrezne ravni informacijske varnosti – zaščite zdravstvenih podatkov pred nepooblaščeno obdelavo – je razviden iz temeljnih pravnih predpisov. Na najbolj splošni ravni to zahteva Splošna uredba o varstvu podatkov (GDPR), Zakon o varstvu osebnih podatkov (ZVOP-2), Zakon o informacijski varnosti (ZInfV), Zakon o kritični infrastrukturi (ZKI), na ravni pravilnikov pa ne smemo spregledati Pravilnika o pogojih, rokih, načinu vključitve in uporabe eZdravja za obvezne uporabnike (Uradni list RS, št. 69/15), ki izrecno določa, da *»obvezni uporabniki eZdravja zagotavljajo varovanje svoje informacijsko-komunikacijske infrastrukture z ukrepi, primernimi glede na tveganja«.*

Med ključne ukrepe, ki zagotavljajo varovanje informacijsko-komunikacijske infrastrukture, sodi šifriranje podatkov. To se izvaja z različnimi mehanizmi, cilj pa je eden: zagotoviti, da se z dejansko vsebino podatkov med prenosom po internetu ne more seznaniti nihče razen pooblaščenih

uporabnikov. Podobno kot programska oprema tudi šifrirni mehanizmi niso določeni enkrat za vselej, ampak jih je treba posodabljati in prilagajati novim varnostnim tveganjem.

Šifriran prenos podatkov med izvajalci zdravstvene dejavnosti in rešitvami eZdravja se izvaja s pomočjo TLS protokola. Na podlagi mednarodnih priporočil sta trenutno varnostno sprejemljivi verziji TLS 1.2 in 1.3. Starejše verzije, TLS 1.0 in 1.1, so izrazito problematične, njihove varnostne ranljivosti so javno znane in jih je zato mogoče sorazmerno enostavno zlorabiti – s tem pa nepooblaščenim osebam omogočiti dostop do občutljivih zdravstvenih podatkov.

V okviru postopnega prehoda iz 32-bitne na novejšo 64-bitno programsko arhitekturo aplikacij za obdelavo zdravstvenih podatkov, ki jo že aktivno spodbujajo različni ponudniki programske opreme, je z vidika varnosti nujno – z vidika stroškov pa zanemarljivo – posodobiti tudi TLS protokol na različico 1.2 ali 1.3.

Dne 15. oktobra 2024 bo NIJZ onemogočil dostop do informacijskih rešitev eZdravja tistim izvajalcem zdravstvene dejavnosti, ki bodo še vedno uporabljali zastarele TLS protokole (verzije nižje od 1.2). Uporaba zastarelih TLS protokolov namreč predstavlja nesprejemljivo varnostno tveganje, ki izvajalce zdravstvene dejavnosti izpostavlja visoki verjetnosti zlorabe zdravstvenih podatkov, kršenju zahtev zgoraj navedene zakonodaje s področja varovanja osebnih podatkov in informacijske varnosti, prav tako pa ogroža stabilnost in varnost nacionalne kritične infrastrukture v zdravstvu.

Pozivamo vas, da to obvestilo posredujete vzdrževalcem svojih informacijskih sistemov, da bodo lahko pravočasno nadgradili varnostne protokole in vam zagotovili nadaljnjo uporabo eZdravja.

Z lepimi pozdravi,

NACIONALNI INŠTITUT ZA JAVNO ZDRAVJE NIJZ 12

doc. dr. Branko Gabrovec
generalni direktor

PO POOBLASTILU
št.: 020-5/2024-1 z dne 7. 2. 2024
mag. Kristina Tratar

Pripravili:
- Matjaž Drev (matjaz.drev@nijz.si)