REPUBLIKA HRVATSKA
MINISTARSTVO ZDRAVSTVA

KLASA: 230-02/25-06/16

URBROJ: 534-06-2-1/1-25-02

Zagreb, 31. ožujka 2025.

UDRUGA POSLODAVACA U ZDRAVSTVU HRVATSKE

Savska cesta 41/VII, 10000 Zagreb

n/p direktora, mr. Dražen Jurković, dr. med. spec.

PREDMET: Osiguranje potrebnih resursa za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima u zdravstvenom sektoru

- **Odgovor na zamolbu, daje se**

(Vaša veza: BROJ: 89/1-9/25 od 18. 3. 2025.)

Poštovani,

Sukladno Uredbi o kibernetičkoj sigurnosti („Narodne novine“, br. 135/2024), kategorizacija subjekata javnog sektora, odnosno razvrstavanje subjekata temeljem Zakona o kibernetičkoj sigurnosti („Narodne novine“, br. 14/2024) je u tijeku, po čijem završetku bi svi razvrstani subjekti trebali primiti obavijest od strane Nacionalnog centra za kibernetičku sigurnost (NCSC-HR) ustrojenog u okviru Sigurnosno-obavještajne agencije (SOA) koja je također, s obzirom na nadležnosti predviđene Zakonom i Uredbom, središnje državno tijelo za kibernetičku sigurnost te nadležno tijelo za vođenje posebnog registra subjekata.

S obzirom na vrstu i broj subjekata u sektorima visoke kritičnosti Zdravstvo i Voda za ljudsku potrošnju te drugim kritičnim sektorima Proizvodnja medicinskih uređaja i *in vitro* dijagnostičkih medicinskih uređaja, Ministarstvo zdravstva nije u mogućnosti pojedinom subjektu pružiti stručnu ili financijsku pomoć.

Upućujemo Vas na dokument „Prioritetne preporuke za zaštitu od kibernetičkih napada“, koju je NCSC-HR objavio na svojim službenim stranicama i namijenio svim subjektima: https://ncsc.hr/UserDocsImages/ostalo/Prioritetne_preporuke_za_zastitu_od_kibernetickih_napada.pdf.

Također, Europska komisija predstavila je Akcijski plan usmjeren na jačanje kibernetičke sigurnosti bolnica i pružatelja zdravstvene zaštite. Akcijski plan je početak procesa poboljšanja kibernetičke sigurnosti u zdravstvenom sektoru te uključuje uspostavu Europskog centra za podršku kibernetičkoj sigurnosti u zdravstvu koji će bolnicama i zdravstvenim ustanovama

Ksaver 200a, 10 000 Zagreb, Republika Hrvatska, T +385 1 46 07 555, F +385 1 46 77 076

pružati prilagođene smjernice, alate, usluge i obuku. Inicijativa se temelji na širem okviru EU-a za jačanje kibernetičke sigurnosti ključne infrastrukture, a ovo je prvi specifični pristup koji koristi sve dostupne EU mjere.

Plan se oslanja na četiri glavna prioriteta: poboljšanu prevenciju, bolju detekciju prijetnji, odgovor na kibernetičke napade te odvraćanje napadača. Specifične mjere postupno će se uvoditi tijekom 2025. i 2026. godine, a rezultati savjetovanja poslužit će za izradu daljnjih preporuka do kraja godine.

Akcijski plan nadovezuje se na postojeći zakonodavni okvir EU-a u području kibernetičke sigurnosti, uključujući NIS2 direktivu koja postavlja zdravstveni sektor kao kritično područje. Novi okvir podupire i Akcijski plan za kibernetičku otpornost te mehanizam solidarnosti EU-a za hitne situacije. Sve ove mjere ključne su za uspostavu Europskog prostora zdravstvenih podataka, kojim će građanima biti omogućena puna kontrola nad njihovim zdravstvenim podacima.

Bolničkim zdravstvenim ustanovama, a i drugim zdravstvenim ustanovama, predlažemo pristupanje sustavu SK@UT, nacionalnom sustavu za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora putem distribuirane mreže senzora i alata za kibernetičku zaštitu. Sustav SK@UT predstavlja dodatnu mjeru kibernetičke zaštite, odnosno ne utječe na obveze koje proizlaze iz Zakona o kibernetičkoj sigurnosti, predstavlja nacionalni „kibernetički kišobran" koji trenutno štiti više od 90 državnih tijela, operatora kritične infrastrukture i pravnih osoba od posebnog interesa za Republiku Hrvatsku. Uz sva ministarstva i druga tijela državne uprave, u SK@UT su uključeni i ključni dijelovi državne informacijske infrastrukture.

U Zakonu o kibernetičkoj sigurnosti SK@UT je naveden kao jedan od dobrovoljnih mehanizama kibernetičke zaštite, čime je omogućeno pristupanje sustavu SK@UT i drugih pravnih osoba u Republici Hrvatskoj. Dobrovoljno pristupanje pravnih osoba sustavu SK@UT provodi se na temelju zahtjeva za pristupanjem sustavu kojeg podnosi pravna osoba, procjene kritičnosti pravne osobe koju provodi NCSC-HR te sporazuma o pristupanju sustavu između NCSC-HR i pravne osobe koja je podnijela zahtjev.

Konačno, Državna škola za javnu upravu (https://www.dsju.hr/) nudi slobodno dostupne programe, poput online programa „Sigurni u kibernetičkom prostoru", čija je svrha podizanje sigurnosne svijesti preventivnim djelovanjem na samosvijest i znanje službenika o raznovrsnim vektorima napada kojima se služe napadači u svom svakodnevnom radu, ili edukacije uživo „Mjere i standardi informacijske sigurnosti u državnim tijelima", s ciljem upoznavanja polaznika s propisima iz područja zaštite tajnosti podataka i informacijske sigurnosti.

S obzirom na sve gore navedeno i raspoloživo za unaprjeđenje kibernetičke sigurnosti, molimo Vas da Vaše potrebe racionalno i svrsishodno iskazujete u redovnoj proceduri planiranja Državnog proračuna za naredno razdoblje.

S poštovanjem,

MINISTRICA

Doc. dr. sc. Irena Hrstić, dr. med.

Dostaviti:

1. Naslovu
2. Arhivi, ovdje

Obavijest o tome:

1. Hrvatski zavod za zdravstveno osiguranje, Margaretska 3. 10000 Zagreb, n/p ravnatelja, Lucian Vukelić, dr. med. spec.