Фонд
здравственог осигурања
Републике Српске

Свим јавним здравственим установама које користе апликације ИЗИС-а

Број: 10/095-199-2/24

Датум: 15.01.2024. године.

Предмет: Примјена нових мјера политике безбједности ИЗИС-а

Поштовани,

У свјетлу недавних догађаја који су утицали на безбједност Интегрисаног Здравственог Информационог Система (ИЗИС), као и у циљу заштите података наших пацијената и интегритета нашег здравственог система, неопходно је унаприједити и појачати мјере политике безбједности.

Заштита осјетљивих здравствених информација и личних података пацијената је наш примарни циљ, те ћемо у наставку овог дописа, детаљно објаснити мјере којима ће се унаприједити и појачати политика безбједности ИЗИС-а.

Желимо нагласити да је сарадња свих здравствених установа у овом процесу од кључног значаја. Разумијемо да ове промјене могу донијети одређене изазове, али смо чврсто увјерени да су ови кораци неопходни за осигурање високог нивоа заштите ИЗИС-а и, што је најважније, заштите података пацијената.

За додатно унапређење безбједности ИЗИС-а, и као одговор на хакерски напад, примјениће се нове мјере безбједоносне заштите, које укључују:

1. Промјена политике лозинке:

- Здравствене установе – администратори ће добити податке са корисничким именима и иницијалном лозинком за све кориснике у оквиру здравствене установе. Администратор је у обавези да појединачно сваком кориснику уручи корисничке креденцијале имајући у виду да су исти подаци лични и тајни.

- Сваки корисник ИЗИС-а ће добити нове приступне податке, укључујући иницијалну лозинку која има 7 карактера, док ће сваку сљедећу лозинку корисник морати унијети са дужином од 15 карактера (најмање 1 мало слово, 1 велико слово, 1 специјални карактер и 1 број).

- Након првог успјешног логовања, корисници су обавезни да промјене своју лозинку. Ово је стандардна пракса за повећање безбједности, јер иницијално генерисане лозинке могу бити привремене или мање сигурне.

Здраве Корде 8
78000 Бања Лука, Република Српска
Босна и Херцеговина

Т: +387 51 249 100
Е: fzors@zdravstvo-srpske.org
www.zdravstvo-srpske.org

ЈИБ: 4400965150008

Желимо обавјестити све кориснике да су параметри за приступ систему (корисничко име и лозинка) лични и тајни подаци те да дијељење истих повлачи за собом одговорност и посљедице.

2. Картица здравственог радника и дигитални потписи:

- Сви постојећи дигитални потписи ће бити замијењени новима. Дигитални потписи су кључни за аутентификацију идентитета корисника.

- Администратори здравствених установа ће морати да прикупе картице са дигиталним потписима од свих запослених и замијене их са новим сертификатима, који ће им бити благовремено прослијеђени. Ово осигурава да су сви корисници у систему ажурирани са најновијим безбједносним стандардима.

3. Хардверске и софтверске измјене на систему:

- Уведене су нове уређаје и софтверске компоненте у ИЗИС, што додатно јача безбједност система против потенцијалних хакерских напада.

- Ове промјене укључују јаче уређаје нове генерације за мрежну безбедност (firewall), унапријеђене механизме антивирусне заштите и друга технолошка побољшања.

4. Примјена антивирус програма:

- Здравствене установе су у обавези да, уколико до сада нису, обавезно користе антивирус програме за своје локалне мреже.

- Све здравствене установе су дужне да врше скенирање својих рачунарских мрежа и радних станица. Циљ је идентификовати и елиминисати потенцијалне безбједносне пријетње унутар мреже или на појединачним рачунарима.

- Ово је важно да би се осигурало да унутрашња инфраструктура није компромитована и да је спремна за имплементацију нових безбједносних политика и протокола.

Напомена:

Подизање степена безбједности, увођењем нових мјера, у пракси може довести до проблема приликом покушаја приступа зараженог система ИЗИС-у. Наиме, у случају да нови механизам безбједоносне заштите ИЗИС-а детектује вирус или неки други штетни програм, који може узроковати проблеме у кориштењу система или оштетити податке, „зараженом“ систему неће бити омогућен приступ ИЗИС-у.

У таквим случајевима, корисници требају прво контактирати администраторе своје здравствене установе, а они да обавијесте администраторе и подршку ИЗИС-а, како би се проблем ријешио.

Молимо све здравствене установе да схвате озбиљност ситуације и да се придржавају нових процедура. Ове промјене су кључне за заштиту и ефикасно функционисање ИЗИС-а и комплетног здравственог система.

Молимо све запослене у здравственим установама да пажљиво прочитају и прате упутства описана у овом допису.

Свјесни смо да је сигурност динамичан процес и зато ћемо наставити да пратимо ситуацију и по потреби уводимо нове мјере.

Захваљујемо вам на вашој посвећености, разумијевању и сарадњи.

За додатне информације и помоћ, слободно нас контактирајте.

С поштовањем,

Извршни директор

за ИТ и опште послове

Драгана Родић, дипл.инж.ел.

по овлашћењу в.д. директора