Република Србија
ВИШИ СУД У КРУШЕВЦУ
I Су 1-39/20
16.10.2020. године
К р у ш е в а ц

На основу члана 8. Закона о информационој безбедности („Службени гласник РС" број 6/2016, 94/2017 и 77/19), члана 2. Уредбе о ближем садржају Акта о безбедности информационо комуникационих система од посебног значаја, начину провере информационо комуникационих система од посебног значаја и садржају извештаја о провери информационог комуникационог система од посебног значаја („Службени гласник РС" број 94/2016) и члана 59. Закона о агенцији за борбу против корупције („Службени гласник РС", број 97/2008, 53/2010, 66/2011, 67/2013, 8/2015, 88/19), председник суда донео је дана 16.10.2020. године

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО КОМУНИКАЦИОНОГ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ВИШЕГ СУДА У КРУШЕВЦУ

УВОДНЕ ОДРЕДБЕ

Члан 1.

Овим Актом уређују се мере заштите од безбедносних ризика у информационо комуникационом систему суда, начин и процедуре постизања и одржавања адекватног нивоа безбедности, овлашћења и одговорности запослених у вези са безбедношћу и ресурсима информационо комуникационе технологије (ИКТ) система суда.

Члан 2.

Поједини термини у смислу Закона о информационој безбедности имају следеће значење:
1) информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:
(1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
(2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
(3) податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
(4) организациону структуру путем које се управља ИКТ системом;
(5) све типове системског и апликативног софтвера и софтверске развојне алате;
2) оператор ИКТ система је правно лице, орган власти или организациона јединица

органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

4) тајност је својство које значи да податак није доступан неовлашћеним лицима;

5) интегритет значи очуваност изворног садржаја и комплетности податка;

6) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

7) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

8) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

9) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

10) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

11) инцидент је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;
11а) јединствени систем за пријем обавештења о инцидентима је информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

12) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

13) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

14) ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

15) орган власти је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења;

16) служба безбедности је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;

17) самостални оператори ИКТ система су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности;

18) компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

19) криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

20) криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

21) криптографски производ је софтвер или уређај путем кога се врши криптозаштита;

22) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

23) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

24) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;

25) услуга информационог друштва је услуга у смислу закона којим се уређује електронска трговина;

26) пружалац услуге информационог друштва је правно лице које је пружалац услуге у смислу закона којим се уређује електронска трговина.

МЕРЕ ЗАШТИТЕ

Члан 4.

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената,

односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се односе на:

1) успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;

2) постизање безбедности рада на даљину и употребе мобилних уређаја;

3) обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност;

4) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;

5) идентификовање информационих добара и одређивање одговорности за њихову заштиту;

6) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;

7) заштиту носача података;

8) ограничење приступа подацима и средствима за обраду података;

9) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;

10 утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију;

11) предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности и интегритета података;

12) физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;

13) заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;

14) обезбеђивање исправног и безбедног функционисања средстава за обраду података;

15) заштиту података и средстава за обраду података од злонамерног софтвера;

16) заштиту од губитка података;

17) чување података о догађајима који могу бити од значаја за безбедност ИКТ система;

18) обезбеђивање интегритета софтвера и оперативних система;

19) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

20) обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;

21) заштиту података у комуникационим мрежама укључујући уређаје и водове;

22) безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;

23) испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;

24) заштиту података који се користе за потребе тестирања ИКТ система односно делова система;

25) заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;

26) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;

27) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;

28) мере које обезбеђују континуитет обављања посла у ванредним околностима.

Влада, на предлог Надлежног органа, ближе уређује мере заштите ИКТ система уважавајући начела из члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

АДМИНИСТРАТОР ИКТ СИСТЕМА

Члан 5.

ИКТ системом управља и руководи запослени који поседује администраторски налог, у складу са описом послова из важећег акта о систематизацији радних места.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Запослено лице које има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог, односно надлежног руководиоца.

Запослени који управља ИКТ системом (администратор) дужан је да сваког новог корисника упозна са одговорностима и правилима коришћења ИКТ ресурса суда и да води евиденцију о изјавама новозапослених корисника да су упознати са правилима коришћења ИКТ ресурса.

Евиденцију о информационим добрима суда води администратор ИКТ система у папирној или електронској форми.

НАЛОЗИ КОРИСНИКА

Члан 6.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира на тај начин што се прво уписује име, па презиме запосленог, која су одвојена тачком и куцају се латиничним писмом без употребе слова Ђ, Ж, Љ, Њ, Ћ, Ч, Џ, Ш.

Уместо ћириличних слова наведених у претходном ставу користе се латиничне ознаке за иста, и то: Ђ- OJ; Ж- 2, Љ-1J, Њ-НJ, Ћ-5, 4-8, Џ-02, Ш-8.

Лозинка корисника мора да садржи минимум осам карактера комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке запосленог.

Ако корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Корисник је дужан да мења лозинку на свака два месеца.

Иста лозинка се не сме понављати у временском периоду од шест месеци.

Члан 7.

Корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору за подешавање корисничког профила и радне станице.

Кориснички налог додељује администратор у сарадњи са непосредним руководиоцем.

За послове извршене под одређеним корисничким именом и лозинком одговоран је корисник ИКТ система коме је корисничко име, тј. налог додељен.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

НАДЗОР И КОНТРОЛА ОД СТРАНЕ АДМИНИСТРАТОРА

Члан 8.

Администратор ИКТ система у обавези је да континуирано надзире и проверава функционисање средстава за обраду података, да управља ризицима који могу утицати на безбедност ИКТ система, као и да планира и предлаже руководиоцу одговарајуће мере.

Администратор ИКТ система је дужан да проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, да врши проверу безбедносних слабости на нивоу техничких карактерстика компоненти ИКТ система, архитектуре решења, техничке конфигурације.

О извршеној провери сачињава извештај и доставља руководиоцу. Извештај треба да садржи време провере, спроведене радње, закључке по питању адекватне примене предвиђених мера заштите, закључке по питању евентуалних безбедносних слабости, оцену стања у погледу информационе безбедности, предлог евентуалних корективних мера, и потпис лица које је спровело проверу ИКТ система.

ПРЕСТАНАК РАДНОГ ОДНОСА ЗАПОСЛЕНОГ И ПРОМЕНА РАДНОГ МЕСТА И ОВЛАШЋЕЊА

Члан 9.

У случају промене радног места, односно овлашћења корисника, администратор ИКТ система ће извршити промену права у коришћењу ИКТ система, у складу са описом радних задатака и захтевом руководиоца корисника.

У случају престанка радног ангажовања корисника, његов кориснички налог се гаси тј. Укида.

О престанку радног односа или радног ангажовања, као и промени радног места корисника, руководилац је дужан да обавести администратора ИКТ система, ради укидања, односно измене приступних налога тог корисника.

Корисник је након престанка правног основа по коме је приступао ресурсима ИКТ система суда, у обавези да не открива податке који су од значаја за информациону безбедност ИКТ система.

ПРЕНОСИВИ МЕДИЈИ И АНТИВИРУСНА ЗАШТИТА

Члан 10.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморијом, CD-ом, итд), инсталацијом нелиценцираног софтвера и слично.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм.

Свакодневно се аутоматски у тачно одређено време врши допуна антивирусних дефиниција.

Забрањено је заустављање и искључивање антивирусног софтвера.

Преносиви медији (USB меморија, CD) пре коришћења морају бити проверени на присуство вируса од стране администратора ИКТ система.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави администратору ИКТ система.

ПОСТУПАЊЕ СА ОПРЕМОМ ИКТ СИСТЕМА

Члан 11.

Простору у коме се налазе сервери, мрежна и комуникациона опрема има право приступа само администратор ИКТ система и ИТ техничар.

У простору је неопходно успоставити и одржавати одговарајућу температуру у складу са важећим стандардима (климатизован простор).

Прозори и врата на просторији из става 1. овог члана морају увек бити затворени и закључани.

Сервер и мрежна опрема (Switch, Modem, Router, Firewall) морају стално бити прикључени на уређаје за непрекидно напајање-UPS.

У случају нестанка електричне енергије у периоду дужем од капацитета UPS-а, администратор ИКТ система је дужан да искључи опрему у складу са процедурама произвођача опреме.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходно стабилну верзију.

Инсталирање новог софтвера, као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запосленог-корисника.

Члан 12.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (Switch, Router) се мора налазити у закључаном Rack орману.

Администратор ИКТ система врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Члан 13.

У случају изношења опреме ИКТ система ради сервисирања, неопходно је писано одобрење руководиоца а по предлогу систем администратора.

Администратор ИКТ система одређује све детаље везане за изношење опреме и сачињава записник у коме се наводи назив и тип опреме, серијски број, назив сервисера.

У случају крајње нужде, у циљу спашавања опреме, иста се може изнети без одобрења руководиоца.

РЕЗЕРВНЕ КОПИЈЕ ПОДАТАКА

Члан 14.

Администратор ИКТ система је у обавези да прави резервне копије база података једном дневно.

Базе података обавезно се архивирају и на преносиве медије (CD-ROM, DVD, USB, екстерни хард диск) једном дневно за потребе обнове базе података.

Недељне, месечне и годишње копије архиве се чувају у просторији која је физички обезбеђена у складу са мерама заиштите од пожара тј. у сефу Вишег суда у Крушевцу.

Месечне копије података се чувају у сефу Вишег суда у Крушевцу, који се налази у приземљу зграде суда.

Исправност копија-архива проверава администратор ИКТ система.

Члан 15.

У случају настанка инцидента, Виши суд у Крушевцу као оператор ИКТ система од посебног значаја поступиће по Уредби о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја.

Члан 16.

Акт о безбедности информационог комуникационог система ступа на правну снагу даном објављивања на огласној табли суда, где ће бити изложен 30 дана, како би се сви запослени упознали са истим.

Акт о безбедности информационог комуникационог система објавити и на интернет страници суда.

ПРЕДСЕДНИК СУДА

Катарина Бошковић