Национална сајбер конференција

2023.

Информациона безбедност
- заједничка одговорност

Уторак
17. октобар
Београд

Хотел
Crowne Plaza
& Онлајн

РАТЕЛ

СРБ-ЦЕРТ

Република Србија
Министарство информисања
и телекомуникација

РНИДС

Нацрт закона о информационој безбедности

Министарство информисања и телекомуникација

Београд, 17. октобар 2023. године

РАТЕЛ

СРБ-ЦЕРТ

Република Србија
Министарство информисања и телекомуникација

РНИДС

Радна група

<u>Општи задатак</u>

- Израда текста Нацрта закона о информационој безбедности

<u>Посебни задаци у оквиру општег</u>

Усклађивање са новим ЕУ легислативним оквиром

Унапређење институционалног и организационог оквира и капацитета

Даља унапређења текста на темељима искуства у примени Закона

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Састав Радне групе

20 органа и организација - 57 члана

Представници државних органа у чијој надлежности су питања од значаја за информациону безбедност: Генерални секретаријат Владе, НБС, Канцеларија Савета за националну безбедност, БИА, Канцеларија за ИТ и електронску управу, МО, ВОА, ВБА, МСП, МУП, РАТЕЛ, Повереник за информације од јавног значаја и заштиту података о личности и МИТ

Представници привреде: ПКС, Савет страних инвеститора

Организације које се баве питањима информационе безбедности: РНИДС, Фондација Мрежа за сајбер безбедност

Образовне институције: Криминалистичко- полицијски универзитет, Правни факултет Универзитета у Новом Саду

Организације које се баве питањима локалне самоуправе: СКГО, НАЛЕД

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

NIS 2 ДИРЕКТИВА

Пун назив: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Усвојена 14. децембра 2022. године

Рок за транспозицију: 17.октобар 2024. године

Предлог упућен у процедуру: 16. децембра 2020. године

NIS 2 ДИРЕКТИВА
Новине у односу на NIS 1

Измене које се односе на секторе према критичности- разликовање између сектора високе критичности и критичних сектора

Ојачана улога ЦЕРТ-ова

Надзор над применом одредби и казнене одредбе

Увођење нових појмова (дефиниција)

Израда националног плана деловања у случају великих инцидената

Одређена тела на нивоу ЕУ која се оснивају на основу овог акта

Редефинисане обавезе оператора система од посебног значаја

Сертификација

Ревидиран приступ дељењу информација о инцидентима и претњама

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

НАЧЕЛА ЗАКОНА

НАЧЕЛО УПРАВЉАЊА РИЗИКОМ

НАЧЕЛО СВЕОБУХВАТНЕ ЗАШТИТЕ

НАЧЕЛО СТРУЧНОСТИ И ДОБРЕ ПРАКСЕ

НАЧЕЛО СВЕСТИ И ОСПОСОБЉЕНОСТИ

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ

ОБЛАСТ	ПОДОБЛАСТ
ЕНЕРГЕТИКА	- производња електричне енергије - комбинована производња електричне и топлотне енергије - снабдевање електричном енергијом - пренос и управљање преносним системом електричне енергије - дистрибуција, управљање дистрибутивним системом и управљање затвореним дистрибутивним системом електричне енергије - складиштење електричне енергије - управљање организованим тржиштем електричне енергије - и друге подобласти предвиђене Законом.

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ

ОБЛАСТ	ПОДОБЛАСТ
САОБРАЋАЈ	- обављање јавног авио-превоза уз важећу оперативну дозволу - управљање аеродромом - услуге контроле летења - управљање јавном железничком инфраструктуром - послови железничких предузећа - обављање превоза путника и терета унутрашњим водама - управљање лукама - управљање бродским саобраћајем (ВТС) - управљање путном инфраструктуром - управљање интелигентним транспортним системима (ИТС)

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ

ОБЛАСТ	ПОДОБЛАСТ
БАНКАРСТВО И ФИНАНСИЈСКА ТРЖИШТА	- послови финансијских институција - послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама - регулисано тржиште - послови клиринга финансијских инструмената - послови пружалаца услуга повезаних с дигиталном имовином

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ

ОБЛАСТ	ПОДОБЛАСТ
ЗДРАВСТВО	- пружање здравствене заштите - рад националних референтних лабораторија - истраживање и развој лекова - производња основних фармацеутских производа и препарата - производња медицинских производа који се сматрају критичним током ванредног стања у области јавног здравља
ВОДА ЗА ПИЋЕ	- снабдевање и дистрибуција воде намењене за људску потрошњу. изузев дистрибутера којима наведени послови нису претежни део њихове делатности
ОТПАДНЕ ВОДЕ	- сакупљање, одвођење или пречишћавање комуналних отпадних вода, отпадних вода насеља и привреде, изузев привредних субјеката којима наведени послови нису претежни део њихове делатности

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ

ОБЛАСТ	ПОДОБЛАСТ
ДИГИТАЛНА ИНФРАСТРУКТУРА	- пружање услуга рачунарства у клауду - пружање услуге центра за чување и складиштење података
УПРАВЉАЊЕ ИКТ УСЛУГАМА КОЈЕ СЕ ПРУЖАЈУ ОПЕРАТОРИМА ПРИОРИТЕТНИХ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА	- пружање управљаних услуга - пружање управљаних безбедносних услуга

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ

ОБЛАСТ	ПОДОБЛАСТ
ДРУГЕ ОБЛАСТИ	- управљање нуклеарним објектима - пружање квалификованих услуга од поверења, пружање услуга ДНС-а, и управљање регистром домена највишег нивоа, са изузетком оператора коренских сервера имена - обављање делатности електронских комуникација - тачка за размену интернет саобраћаја - области у којој у Републици Србији постоји само један пружалац услуге и која је неопходна за обављање критичних друштвених и привредних делатности

Оператори ИКТ система од посебног значаја ПРИОРИТЕТНИ органи власти и критична инфраструктура

ОРГАНИ ВЛАСТИ И КРИТИЧНА ИНФРАСТРУКТУРА
- државни орган, орган аутономне покрајине, јединица локалне самоуправе организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења - оператори критичне инфраструктуре у складу са законом којим се уређује критична инфраструктура

Оператори ИКТ система од посебног значаја ВАЖНИ

ОБЛАСТ
- поштанске услуге у смислу закона којим се уређује област поштанских услуга - управљање отпадом, у смислу закона којим се уређује управљање отпадом, изузев привредних субјеката којима наведени посао није претежни део њихове делатности - производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије - производња, обрада и дистрибуција хране у сегменту велепродаје и индустријске производње и прераде - производња рачунара, електронских и оптичких производа - производња електричне опреме - производња машина и уређаја - производња моторних возила, приколица и полуприколица и производња остале опреме за превоз - и друге области одређене Законом.

Обавезе оператора ИКТ система од посебног значаја

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА:

1) се упише у евиденцију ИКТ система од посебног значаја;
2) предузме одговарајуће техничке, оперативне,организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената;
3) изврши процену ризика и донесе акт о процени ризика;
4) донесе акт о безбедности ИКТ система од посебног значаја;
5) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система и то најмање два пута годишње (важи за приоритетне ИКТ системе, важни ИКТ системи проверу обављају најмање једном годишње);
6) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја са трећим лицима;
7) доставља обавештења, без одлагања, о сваком инциденту који је значајно угрозио безбедност ИКТ систем од посебног значаја;
8) доставља обавештења о озбиљним претњама за ИКТ систем од посебног значаја;
9) достави статистичке податке о инцидентима и избегнутим инцидентима у ИКТ системима.

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Самостални оператори

Самостални оператори	Дужности
▪ Министарство одбране ▪ Министарство унутрашњих послова ▪ Министарство спољних послова ▪ Службе безбедности ▪ Народна банка Србије	1) се упише у евиденцију ИКТ система од посебног значаја
	2) предузме одговарајуће техничке, оперативне, организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената
	3) донесе акт о безбедности ИКТ система
	4) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система у складу са сопственим правилима за проверу усклађености мера заштите
	5) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја са трећим лицима
	6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима.

Евиденција ИКТ система од посебног значаја

ПОДАЦИ
- назив, матични број и седиште оператора ИКТ система од посебног значаја; - име и презиме, службена адреса за пријем електронске поште и службени контакт телефон администратора ИКТ система од посебног значаја; - име и презиме, службена адреса за пријем електронске поште и службени контакт телефон одговорног лица ИКТ система од посебног значаја; - податак о врсти ИКТ система од посебног значаја, односно да ли ИКТ систем од посебног значаја потпада под приоритетан или важан; - податак о делатности оператора ИКТ система од посебног значаја; - адресни опсег интернет протокола (енгл. „ip address range“) који припадају ИКТ систему од посебног значаја; - веб страница оператора ИКТ система од посебног значаја; - број локација на којима се ИКТ систем од посебног значаја налази.

Мере заштите

Оператори ИКТ система од посебног значаја треба да предузму мере које се односе на:

Техничке

Организационе

Оперативне

Акт о процени ризика

ПРОЦЕНА РИЗИКА
• врши се процена ризика за ИКТ систем од посебног значаја с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај • ревидира се једном годишње • израђује се у складу са општом методологијом за процену ризика у ИКТ системима од посебног значаја

Акт о безбедности ИКТ система

ОБАВЕЗА ДОНОШЕЊА АКТА О БЕЗБЕДНОСТИ
• Актом о безбедности одређују се мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Провера усклађености мера заштите

УЧЕСТАЛИЈЕ ПРОВЕРЕ
- оператор приоритетног ИКТ система од посебног значаја дужан је да, самостално или уз ангажовање спољних експерата, врши проверу усклађености примењених мера ИКТ система - оператори приоритетних ИКТ система од посебног значаја врше проверу усклађености најмање двапут годишње, док оператори важних ИКТ система врше проверу најмање једном годишње.

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

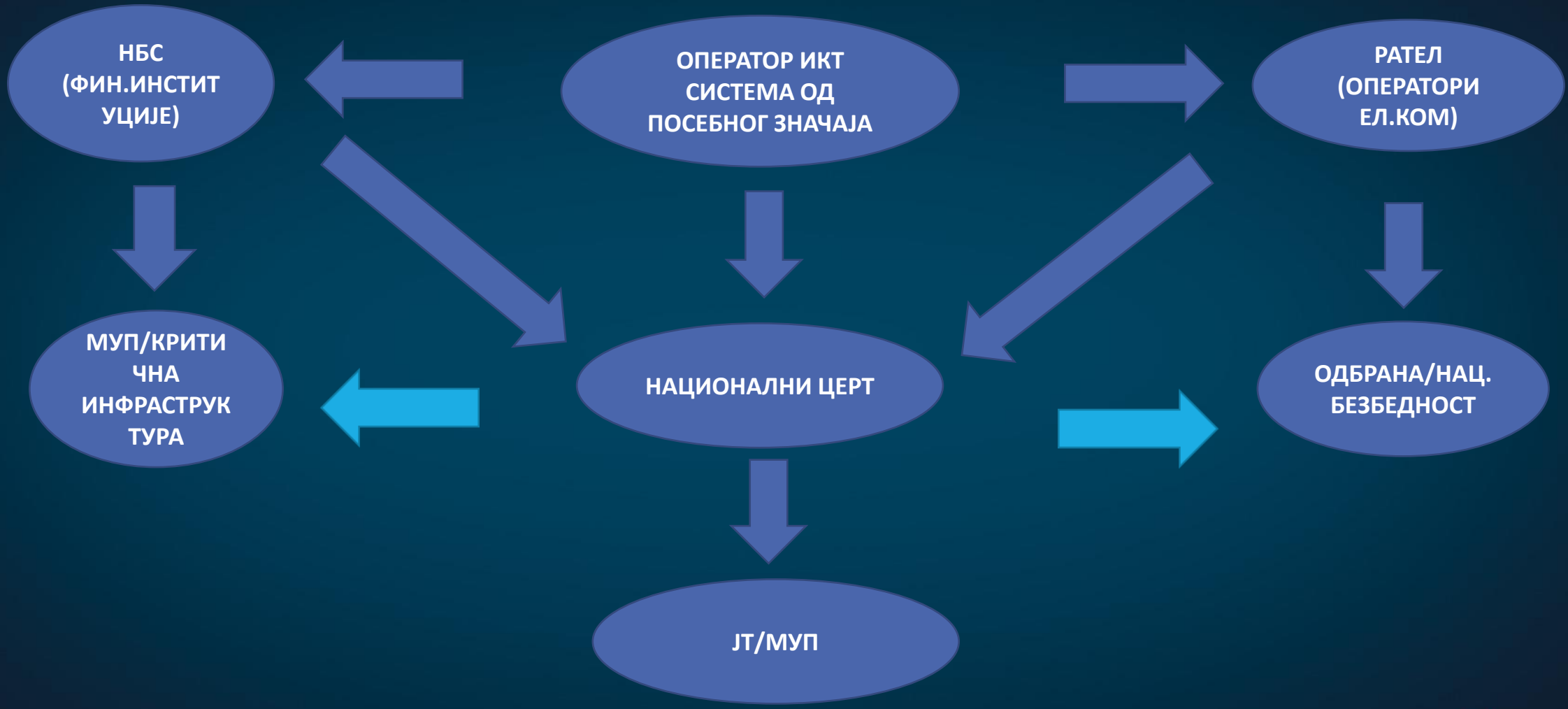
Обавештавање о инцидентима који значајно угрожавају информациону безбедност

ОПЕРАТОРИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖНИ СУ ДА:

- пријаве инцидент без одлагања, а најкасније у року од 24 сата од када су сазнали за инцидент
- пријаву изврше путем јединственог система за пријем обавештења о инцидентима обавесте о инциденту кориснике којима пружају услуге, без одлагања, у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга, као и о мерама које корисници могу да предузму и употребе у циљу умањења или елиминације штетних последица инцидента
- током инцидента достављају обавештења и додатне извештаје о битним догађајима у вези са инцидентом и активностима које предузимају
- у року од 15 дана од дана престанка инцидента доставе завршни извештај о инциденту
- финансијске институције, Кредитни биро и пружаоци услуга повезаних с дигиталном имовином изузетно обавештавају НБС, а оператори електронских комуникација РАТЕЛ

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Обавештавање о инцидентима који значајно угрожавају информациону безбедност



РАТЕЛ

СРБ-ЦЕРТ

Република Србија
Министарство информисања и телекомуникација

РНИДС

Инциденти који могу да имају значајан утицај на нарушавање информационе безбедности оператора ИКТ система од посебног значаја

ОПЕРАТОР МОРА ДА ПРИЈАВИ СЛЕДЕЋЕ ИНЦИДЕНТЕ:

- инциденте који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга
- инциденте који утичу на велики број корисника услуга, или трају дужи временски период
- инциденте који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност
- инциденте који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије
- инциденте који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе
- инциденте који су настали као последица инцидента у ИКТ систему из члана 5. став 2. тачка 1) подтачка (7) овог закона (дигитална инфраструктура – рачунарство у клауду и центар за чување и складиштење података), када ИКТ систем од посебног значаја у свом пословању користи информационе услуге ИКТ система из члана 5. став 2. тачка 1) подтачка (7) овог закона
- инциденте који изазивају или могу да изазову знатну материјалну или нематеријалну штету оператору ИКТ система од посебног значаја и другим физичким и правним лицима

Значај инцидента према нивоу опасности

НИВО	ОРГАНИ КОЈИ УПРАВЉАЈУ ОДГОВОРОМ НА ИНЦИДЕНТ
ВЕОМА ВИСОК (КРИЗА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ)	Влада проглашава стање кризе информационе безбедности и задужује органе да поступају по предложеним мерама у складу са својим надлежностима.
ВИСОК	Управљање инцидентима високог, средњег и ниског нивоа води Канцеларија за информациону безбедност (Национални ЦЕРТ) у сарадњи са операторима ИКТ система од посебног значаја, министарством надлежним за послове информационе безбедности, Телом за координацију информационе безбедности и другим надлежним органима по потреби
СРЕДЊИ	
НИЗАК	

Статистички подаци о инцидентима

ПОДАЦИ КОЈИ СЕ ДОСТАВЉАЈУ:
Оператор ИКТ система од посебног значаја дужан је да достави Националном ЦЕРТ-у статистичке податке о свим инцидентима у ИКТ систему, укључујући и избегнуте инциденте, у претходној години најкасније до 28. фебруара текуће године. Национални ЦЕРТ извештаје о статистичким подацима доставља министарству надлежном за послове информационе безбедности . Врсту, форму и начин достављања статистичких података утврђује Национални ЦЕРТ.

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Институционални оквир

ИНСТИТУЦИЈА	НАДЛЕЖНОСТИ
МИНИСТАРСТВО ИНФОРМИСАЊА И ТЕЛЕКОМУНИКАЦИЈА	• Надлежни орган за информациону безбедност (прописи, плански документи, инспекцијски надзор)
КАНЦЕЛАРИЈА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ	• ЦЕРТ органа, Национални ЦЕРТ (након транзиционог периода), јединствена тачка контакта, управљање инцидентима, минималне мере заштите органа
МИНИСТАРСТВО ОДБРАНЕ	• Одобравање криптографских производа који се користе за руковање тајним подацима • Дистрибуција криптоматеријала • Заштита од КЕМЗ

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Канцеларија за информациону безбедност

КАНЦЕЛАРИЈА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ

Оснива се ради обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији и има следеће надлежности:

- управљање инцидентима који значајно угрожавају информациону безбедност
- обавља послове Националног ЦЕРТ-а (након транзиционог периода)
- обавља послове ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе
- сарадњу на националном нивоу у области информационе безбедности
- послове јединствене тачке контакта
- послове стандардизације и сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга
- прописује минималне мере заштите ИКТ система органа
- у сарадњи са надлежним органима учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима
- извештава Министарство на кварталном нивоу о предузетим активностима
- друге послове у складу са овим законом

Послови Националног ЦЕРТ-а

НАЦИОНАЛНИ ЦЕРТ

- прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система, прати стање о инцидентима у Републици Србији, пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима;
- реагује без одлагања по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања;
- на захтев оператора ИКТ система од посебног значаја, пружа помоћ у праћењу стања безбедности ИКТ система у реалном времену или приближно реалном времену;
- на захтев оператора ИКТ система од посебног значаја, врши проактивно скенирање ИКТ система у циљу утврђивања рањивости које могу да потенцијално знатно наруше безбедност ИКТ система, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора;
- поступа као координатор за потребе координираног откривања рањивости, у складу са овим законом, учествује у развоју и коришћењу технолошких алата за размену информација
- континуирано израђује анализе ризика и инцидената, на основу прикупљених информација, подиже свест код грађана, привредних субјекта и органа о значају информационе безбедности

База рањивости

БАЗА РАЊИВОСТИ
- Национални ЦЕРТ успоставља и одржава базу рањивости ИКТ производа и ИКТ услуга у Републици Србији и омогућава физичким и правним лицима, као и произвођачима, добављачима и пружаоцима услуге у ИКТ систему, да на добровољној бази пријаве рањивости у ИКТ производима или ИКТ услугама, а које се могу пријавити анонимно. **База рањивости ИКТ производа и ИКТ услуга садржи:** - податке о рањивости; - податке о ИКТ производима или ИКТ услугама на које рањивост утиче.

Међународна сарадња и послови јединствене тачке контакта

МЕЂУНАРОДНА САРАДЊА

Национални ЦЕРТ остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

- брзо расту или имају тенденцију да постану високоризични;
- превазилазе или могу да превазиђу националне капацитете;
- могу да имају негативан утицај на више од једне државе.

Национални ЦЕРТ обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.

ЦЕРТ мреже електронске управе

ЦЕРТ мреже електронске управе обавља следеће послове:

- врши заштиту мреже еУправе
- обавља координацију и сарадњу са операторима ИКТ система које повезује мрежа еУправе у превенцији инцидената
- активно учествује у откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената
- врши проактивно скенирање мреже
- у случају откривене рањивости обавести операторе ИКТ система који су корисници мреже еУправе о томе и налаже операторима ИКТ система од посебног значаја који су корисници мреже да предузму адекватне мере заштите у циљу спречавања, смањења и отклањања последица индицента
- издаје стручне препоруке за заштиту ИКТ система органа, осим ИКТ система за рад са тајним подацима, прописује процедуре за поступање оператора ИКТ система од посебног значаја који користе мреже у случају инцидента
- и друге послове предвиђене Законом.

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Национални контакт центар за безбедност деце на интернету

БЕЗБЕДНОСТ ДЕЦЕ НА ИНТЕРНЕТУ
Министарство предузима превентивне мере за безбедност и заштиту деце на интернету, као активности од јавног интереса, путем едукације и информисања деце, родитеља и наставника о предностима, ризицима и начинима безбедног коришћења интернета, као и путем јединственог места за пружање савета и пријем пријава у вези безбедности деце на интернету, и упућује пријаве надлежним органима ради даљег поступања.

РАТЕЛ

СРБ-ЦЕРТ

Република Србија
Министарство информисања и телекомуникација

РНИДС

Криптобезбедност и заштита од КЕМЗ

МИНИСТАРСТВО ОДБРАНЕ
• врши функцију националног органа за одобрење криптопроизвода и заштиту од КЕМЗ • развија, имплементира, верификује и класификује криптографске алгоритме и производе и решења заштите од КЕМЗ • научноистраживачки рад; • национални орган за дистрибуцију криптоматеријала; • предлаже доношење прописа из области криптобезбедности и заштите од КЕМЗ на основу овог закона; • врши послове стручног надзора у вези криптобезбедности и заштите од КЕМЗ

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Одобрење за криптографски производ

ТАЈНИ ПОДАЦИ У ИКТ СИСТЕМИМА
• Криптографски производи који се користе за заштиту преноса и чувања података који су одређени као тајни, у складу са законом, морају бити верификовани и одобрени за коришћење. • **ОПШТЕ ОВЛАШЋЕЊЕ** – самостални оператори (не треба одобрење)

Инспекција за информациону безбедност

НАДЗОР НАД ОПЕРАТОРИМА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом:

1) наложи отклањање утврђених неправилности и за то утврди разуман рок
2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок
3) захтева од оператора ИКТ система од посебног значаја да изврши скенирање мреже у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика
4) наложи да надзирани субјект учини доступним јавности информације које се тичу непоштовања одредби овог закона, а за које постоји оправдан интерес јавности на утврђени начин
5) наложи да надзирани субјект одреди лице са тачно утврђеним овлашћењима које ће у утврђеном временском периоду надзирати и пратити усаглашеност са одредбама овог закона и наложеним мерама.

РАТЕЛ СРБ-ЦЕРТ Република Србија Министарство информисања и телекомуникација РНИДС

Важење претходног закона

ПРИМЕНА ПРЕТХОДНОГ ЗАКОНА ДО ДОНОШЕЊА НОВИХ ПОДЗАКОНСКИХ АКАТА
Даном ступања на снагу овог закона престаје да важи Закон о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19), изузев одредби које се односе на обавезе оператора ИКТ система од посебног значаја које важе до доношења подзаконског акта који уређује критеријуме за операторе ИКТ система од посебног значаја. Подзаконски акти донети на основу Закона о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) примењиваће се до доношења подзаконских аката у складу са овим законом.

ХВАЛА НА ПАЖЊИ!

milan.vojvodic@mit.gov.rs

РАТЕЛ

СРБ-ЦЕРТ

Република Србија
Министарство информисања и телекомуникација

РНИДС