На основу члана 11. став 9. Закона о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) и члана 42. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС, 44/14 и 30/18 – др. закон),

Влада доноси

УРЕДБУ

о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја

Предмет Уредбе

Члан 1.

Овом уредбом уређује се поступак обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја (у даљем тексту: ИКТ системи од посебног значаја) који могу да имају значајан утицај на нарушавање информационе безбедности.

Уредбом се уређује и листа, врсте и значај инцидената према нивоу опасности, као и поступање и размена информација о инцидентима између органа чији су представници именовани у Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију).

Поступак обавештавања о инцидентима

Члан 2.

Оператори ИКТ система од посебног значаја достављају обавештења о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности без одлагања, а најкасније наредног радног дана од дана сазнања о настанку инцидента, у складу са законом.

Обавештења о инцидентима достављају се преко веб странице министарства надлежног за информациону безбедност (у даљем тексту: Министарство) или Националног центра за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) у јединствени систем за пријем обавештења о инцидентима (у даљем тексту: јединствени систем) којег одржава Министарство.

Оператори ИКТ система од посебног значаја који обављају послове финансијских институција и послове вођења регистра података о обавезама физичких и правних лица према финансијским институцијама обавештења о инцидентима достављају Народној банци Србије, без одлагања, најкасније наредног радног дана од дана сазнања о настанку инцидента.

Оператори ИКТ система од посебног значаја који обављају делатности у области електронских комуникација обавештења о инцидентима достављају регулаторном телу за електронске комуникације (у даљем тексту: РАТЕЛ), без одлагања, најкасније наредног радног дана од дана сазнања о настанку инцидента.

Народна банка Србије и РАТЕЛ примљена обавештења из ст. 3. и 4. овог члана достављају у јединствени систем, без одлагања, а најкасније наредног радног дана од дана пријема тих обавештења, у складу са законом.

Органи који, у складу са овом уредбом, поступају у случају инцидената у ИКТ системима од посебног значаја и размењују податке о тим инцидентима дужни су да обезбеде заштиту података о тим инцидентима у складу са прописима и да те податке користе искључиво у сврху за коју су прибављени.

Садржај обавештења о инциденту

Члан 3.

Обавештење о инциденту мора да садржи следеће податке:

1) назив подносиоца пријаве, број телефона и адреса електронске поште,

2) врсту и опис инцидента,

3) датум и време почетка инцидента и трајање инцидента,

4) последице које је инцидент изазвао,

5) предузете активности ради ублажавања последица инцидента,

6) по потреби, друге релевантне информације.

У случају хитности обавештење о инциденту се додатно пријављује телефонским путем, путем електронске поште или на други одговарајући начин.

Министарство, Народна банка Србије и РАТЕЛ могу ближе уредити поступак обавештавања о инцидентима, у складу са овом уредбом.

Листа инцидената према врстама

Члан 4.

Врсте инцидената у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности сврставају се у групе инцидената, у складу са Листом инцидената према врстама која је дата у Прилогу 1. који је одштампан уз ову уредбу и чини њен саставни део.

Значај инцидената

Члан 5.

Инциденти у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности сврставају се према нивоу опасности, имајући у виду последице инцидента, у складу са Класификацијом инцидента према нивоу опасности (у даљем тексту: Класификација) која је дата у Прилогу 2. који је одштампан уз ову уредбу и чини њен саставни део.

Прикупљање, анализа и размена информација о ризицима за безбедност ИКТ система

Члан 6.

По пријему обавештења о инциденту у ИКТ систему од посебног значаја, Национални ЦЕРТ поступа у складу са надлежностима утврђеним законом, односно прикупља, анализира и размењује информације о ризицима за безбедност ИКТ система, као и инциденту, и у вези тога обавештава, пружа подршку, упозорава и саветује оператора ИКТ система од посебног значаја и врши друге послове из своје надлежности.

Национални ЦЕРТ, након извршене анализе, утврђује ниво опасности од инцидента, у складу са Класификацијом инцидената према значају нивоа опасности (Прилог 2).

Упозоравање и саветовање јавности о инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности ИКТ система од посебног значаја у Републици Србији, Национални ЦЕРТ предузима након добијене сагласности Министарства.

Поступање у случају инцидента који је везан за извршење кривичног дела, угрожавање одбране Републике Србије или угрожавање националне безбедности

Члан 7.

Органи из члана 2. ове уредбе без одлагања достављају обавештења о инцидентима надлежним органима, у складу са законом, ако је инцидент повезан са:

1) извршењем кривичних дела која се гоне по службеној дужности,

2) значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање одбране Републике Србије,

3) значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање националне безбедности.

Поступање у случају инцидента нивоа опасности „веома висок”

Члан 8.

У случају инцидента којем је у складу са Класификацијом утврђен ниво опасности „веома висок” Национални ЦЕРТ без одлагања обавештава о томе Министарство које потом обавештава Републички штаб за ванредне ситуације који поступа у складу са надлежностима утврђеним прописима.

У случају инцидента из става 1. овог члана Министарство сазива седницу Тела за координацију.

Током трајања инцидента Национални ЦЕРТ редовно обавештава Министарство и Тело за координацију о предузетим активностима, а по завршетку инцидента доставља извештај о исходу инцидента најкасније у року од три дана, путем јединственог система.

Поступање у случају инцидента нивоа опасности „висок”

Члан 9.

У случају инцидента којем је у складу са Класификацијом утврђен ниво опасности „висок” Национални ЦЕРТ без одлагања обавештава о томе Министарство које потом сазива седницу Тела за координацију.

Национални ЦЕРТ сазива састанак са представницима Министарства, ЦЕРТ-а органа власти и ЦЕРТ-овима самосталних оператора ради међусобне координације током реаговања по пријављеном инциденту, а у складу са надлежностима.

По потреби, састанцима из става 2. овог члана присуствују и представници посебних ЦЕРТ-ова, као и друга лица.

У случају да је неопходно, инспектор за информациону безбедност може да забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност у ИКТ систему од посебног значаја и за то остави рок, у складу са законом.

Током трајања инцидента Национални ЦЕРТ редовно обавештава Министарство и Тело за координацију о предузетим активностима, а по завршетку инцидента доставља извештај о инциденту најкасније у року од три дана, путем јединственог система.

По извршеној процени, Министарство може да обавести јавност о инциденту, или дати сагласност Националном ЦЕРТ-у за обавештавање јавности.

Поступање у случају инцидента нивоа опасности „средњи”

Члан 10.

У случају инцидента којем је у складу са Класификацијом утврђен ниво „средњи” Национални ЦЕРТ без одлагања обавештава о томе Министарство које потом, у случају да се процени да је потребно, сазива седницу Тела за координацију.

Национални ЦЕРТ припрема предлог препорука за поступање и ступа у контакт са ИКТ системом од посебног значаја у коме се десио инцидент у циљу примене предложених препорука за поступање.

Током трајања инцидента Национални ЦЕРТ редовно обавештава Министарство о предузетим активностима, а по завршетку инцидента доставља извештај о инциденту најкасније у року од три дана, путем јединственог система.

По извршеној процени, Министарство може обавестити јавност о инциденту, или дати сагласност Националном ЦЕРТ-у за обавештавање јавности.

Поступање у случају инцидента нивоа опасности „низак”

Члан 11.

У случају инцидента којем је у складу са Класификацијом утврђен ниво опасности „низак” Национални ЦЕРТ обавештава о томе Министарство.

Национални ЦЕРТ по потреби припрема предлог препорука за поступање и ступа у контакт са ИКТ системом од посебног значаја у коме се десио инцидент.

Током трајања инцидента Национални ЦЕРТ редовно обавештава Министарство о предузетим мерама, а по завршетку инцидента доставља извештај о инциденту најкасније у року од три дана, путем јединственог система.

Престанак важења ранијег прописа

Члан 12.

Даном ступања на снагу ове уредбе престаје да важи Уредба о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Службени гласник РС”, број 94/16).

Завршна одредба

Члан 13.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

05 број 110-364/2020-1

У Београду, 6. фебруара 2020. године

Влада

Председник,

Ана Брнабић, с.р.

Прилог 1.

ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА	
Група инцидената	**Врста инцидента**
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. „malware”)	Вирус
	Црв (енгл. „worm”)
	Рансомвер (енгл. „ransomware”)
	Тројанац
	Шпијунски софтвер (енгл. „spyware”)
	Руткит (енгл. „rootkit”)
Неовлашћено прикупљање података	Скенирање портова
	Пресретање података између рачунара и сервера (енгл. „sniffing”)
	Социјални инжењеринг (лажно представљање и други облици)
	Компромитовање или цурење података (енгл. „data breaches”)
Превара	Фишинг (енгл. „phishing”)
	Неовлашћено коришћење ресурса (енгл. „cryptojacking” и други облици)
Покушаји упада у ИКТ систем	Покушај искоришћавања рањивости система
	Покушај откривања креденцијала (енгл. „brute force attack”, „dictionary attack” и сл.)
Упад у ИКТ систем	Откривање или неовлашћено коришћење привилегованих налога (енгл. „privileged account compromise”)
	Откривање или неовлашћено коришћење непривилегованих налога (енгл. „unprivileged account compromise”)
	Неовлашћени приступ апликацији
	Мрежа заражених уређаја (енгл. „botnet”)

ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА	
Група инцидената	**Врста инцидента**
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. „denial-of-service attack” – DoS)
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. „distributed denial-of-service attack” – DDoS)
	Саботажа
	Прекид у функционисању система или дела система (енгл. „outage”)
Угрожавање безбедности података	Неовлашћен приступ подацима
	Неовлашћена измена или брисање података
	Криптографски напад
Оперативни инциденти	Отказивање хардверских компоненти
	Проблеми у раду са софтверским компонентама
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти
	Пожар
	Поплава
Остали инциденти	Инциденти који не спадају у горе наведене категорије

Прилог 2.

КЛАСИФИКАЦИЈА ИНЦИДЕНТА ПРЕМА НИВОУ ОПАСНОСТИ	
Ниво опасности	**Последице инцидента**
Веома висок	У случају наступања околности угрожавања, ометања рада или онемогућавања рада ИКТ система од посебног значаја, а када су ризици, претње или настале последице инцидента по становништво, материјална добра или животну средину таквог обима и интензитета да њихов настанак или последице није могуће спречити или отклонити редовним деловањем надлежних органа и служби, због чега је за њихово ублажавање и отклањање неопходно употребити посебне мере, додатне снаге и средства уз појачан режим рада.
Висок	Када су ризици и претње или настале последице инцидента по становништво, материјална добра или животну средину таквог обима и интензитета да је њихов настанак или последице могуће спречити или отклонити редовним деловањем надлежних органа и служби.
Средњи	Када су ризици, претње или настале последице инцидента таквог обима и интензитета да могу бити отклоњена заједничким деловањем ИКТ система од посебног значаја у коме се инцидент десио и Националног ЦЕРТ-а.
Низак	Када су ризици, претње или настале последице инцидента таквог обима и интензитета да могу бити отклоњене деловањем ИКТ система од посебног значаја.