Н А Ц Р Т

На основу члана 23. став 1. Закона о електронским комуникацијама („Службени гласник РС“, бр. 44/10, 60/13-УС, 62/14 и 95/18-др.закон), члана 11б. став 3. Закона о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) и члана 16. тачка 4) Статута Регулаторне агенције за електронске комуникације и поштанске услуге („Службени гласник РС“, бр.125/14 и 30/16),

Управни одбор Регулаторне агенције за електронске комуникације и поштанске услуге, као надлежне за послове Националног центра за превенцију безбедносних ризика у информационо-комуникационим системима, на ____седници трећег сазива одржаној дана_____ године, доноси

ПРАВИЛНИК

о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја

I. Уводне одредбе

Члан 1.

Овим правилником ближе се прописују врста, форма и начин достављања статистичких података о свим инцидентима у информационо-комуникационим системима (у даљем тексту: ИКТ системи) од посебног значаја уписаних у евиденцију оператора ИКТ система од посебног значаја (у даљем тексту: Евиденција), на годишњем нивоу.

II. Врста статистичких података

Члан 2.

Врста статистичких података о свим инцидентима у ИКТ систему од посебног значаја утврђена је у обрасцу ИСП - ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА (у даљем тексту: Образац ИСП), који је одштампан уз овај правилник и чини његов саставни део.

Образац ИСП из става 1. овог члана садржи податке о оператору ИКТ система од посебног значаја и листу инцидената према врстама.

Подаци о оператору ИКТ система од посебног значаја односе се на: пуно пословно име оператора, седиште оператора, адресу за контакт, матични број, овлашћено лице, контакт особу, телефон контакт особе, e-mail контакт особе, интернет страницу и укупан број IP уређаја.

Листа инцидената према врстама садржи групе инцидената, врсте инцидената у оквиру те групе и број инцидената, и то:

1) Инсталирање злонамерног софтвера у оквиру ИКТ система: малвер (енгл. *malware*), вирус, црв (енгл. *worm*), рансомвер (енгл. *ransomware*), Тројанац, шпијунски софтвер (енгл. *spyware*) и руткит (енгл. *rootkit*);
2) Неовлашћено прикупљање података: скенирање портова, пресретање података између рачунара и сервера (енгл. *sniffing*), социјални инжењеринг (лажно представљање и други облици) и повреда података (енгл. *data breaches*);
3) Превара: фишинг (енгл. *phishing*) и неовлашћено коришћење ресурса (енгл. *cryptojacking* и други облици);
4) Покушаји упада у ИКТ систем: покушај искоришћавања рањивости система и покушај откривања налога (енгл. *brute force attack*);
5) 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 и мрежа ботова (енгл. *botnet*);
6) Недоступност или ограничена доступност ИКТ система: напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack* – DoS), вишеструки напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack* – DDoS), саботажа и прекид у функционисању система или дела система (енгл. *outage*);
7) Угрожавање безбедности података: неовлашћени приступ подацима, неовлашћена измена података и криптографски напад;
8) Остали инциденти, односно инциденти који не спадају у горе наведене категорије.

III. Форма и начин достављања статистичких података

Члан 3.

Оператори ИКТ система од посебног значаја тачне статистичке податаке о свим инцидентима у ИКТ систему достављају електронским путем, односно попуњавањем Обрасца ИСП на интернет страници Националног центра за превенцију безбедносних ризика у информационо-комуникационим системима (у даљем тексту: Национални ЦЕРТ).

Оператори ИКТ система од посебног значаја су дужни да Образац ИСП попуњен са статистичким подацима о свим инцидентима у ИКТ систему од посебног значаја за претходну годину доставе најкасније до 28. фебруара текуће године.

IV. Поступање и руковање достављеним статистичким подацима

Члан 4.

Обраду статистичких података, који су достављени у складу са начином прописаним чланом 3. овог правилника, Национални ЦЕРТ врши према врсти инцидената, као и према другим критеријумима који су од значаја за сагледавање стања о безбедносним ризицима и инцидентима на националном нивоу.

Национални ЦЕРТ обједињује статистичке податке из става 1. овог члана у форми Годишњег извештаја који доставља министарству надлежном за послове информационе

безбедности (у даљем тексту: Надлежни орган) и исти објављује на својој интернет страници најкасније до краја другог тромесечја текуће године.

Члан 5.

Појединачни подаци о операторима ИКТ система од посебног значаја из достављеног Извештаја о статистичким подацима не могу се јавно објављивати.

Појединачни подаци из Обрасца ИСП не могу се уступати трећим лицима без изричите сагласности оператора ИКТ система од посебног значаја.

Сагласност из става 2. овог члана даје се у форми писане изјаве законског заступника оператора ИКТ система од посебног значаја.

Члан 6.

Статистички подаци достављени након 28. фебруара текуће године неће бити садржани у Годишњем извештају Националног ЦЕРТ-а.

Листу оператора ИКТ система од посебног значаја који нису доставили податке у складу са начином прописаним чланом 3. овог правилника, Национални ЦЕРТ доставља Надлежном органу најкасније до краја другог тромесечја текуће године.

V. Завршна одредба

Члан 7.

Овај правилник објављује се у „Службеном гласнику Републике Србије“ и ступа на снагу осмог дана од дана објављивања.

ПРЕДСЕДНИК
УПРАВНОГ ОДБОРА

Драган Ковачевић

Број:

У Београду, ------2020. године

Образац ИСП

ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА

ПОДАЦИ О ОПЕРАТОРУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

Пуно пословно име оператора	
Седиште оператора	
Адреса за контакт	
Матични број	
Овлашћено лице	
Контакт особа	
Телефон контакт особе	
E-mail контакт особе	
Интернет страница	
Укупан број IP уређаја*	

*уписати укупан број свих уређаја који користе IP протокол за комуникацију

ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА

Група инцидената	Врста инцидента	Број инцидената
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*)	

Група инцидената	Врста инцидента	Број инцидената
Неовлашћено прикупљање података	Скенирање портова	
	Пресретање података између рачунара и сервера (енгл. *sniffing*)	
	Социјални инжењеринг (лажно представљање и други облици)	
	Повреда 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 налога (енгл. *brute force attack*)	
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 ботова (енгл. *botnet*)	
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack* – DoS)	
	Вишеструки напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack* – DDoS)	
	Саботажа	

Група инцидената	Врста инцидента	Број инцидената
	Прекид у функционисању система или дела система (енгл. *outage*)	
Угрожавање безбедности података	Неовлашћен приступ подацима	
	Неовлашћена измена података	
	Криптографски напад	
Остали инциденти	Инциденти који не спадају у горе наведене категорије	

У Београду, дана _____

О б р а з л о ж е њ е

I. Правни основ

Правни основ за доношење Правилника о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја (у даљем тексту: Правилник), садржан је у одредби члана 23. став 1. Закона о електронским комуникацијама („Службени гласник РС“, бр. 44/10, 60/13-УС, 62/14 и 95/18-др. закон, у даљем тексту: ЗЕК). Одредбом члана 23. став 1. ЗЕК-а прописано је да Управни одбор Регулаторне агенције за електронске комуникације и поштанске услуге (у даљем тексту: Агенција) доноси правилнике, упутства, одлуке и друга акта којима се на општи начин уређују питања из надлежности Агенције.

Одредбом члана 11б. став 3. Закона о информационој безбедности („Службени гласник РС“, бр. 6/16, 94/17 и 77/19, у даљем тексту: Закон) је утврђено да Национални центар за превенцију безбедносних ризика у информационо-комуникационим системима (у даљем тексту: Национални ЦЕРТ) утврђује врсту, форму и начин достављања статистичких података о свим инцидентима у ИКТ систему.

II. Разлози за доношење Правилника

Ступањем на снагу Закона о изменама и допунама Закона о информационој безбедности („Службени гласник РС, број 77/19) установљено је овлашћење Националног ЦЕРТ-а, односно Агенције, да донесе подзаконски акт којим ће прописати врсту, форму и начин достављања статистичких података о свим инцидентима у ИКТ систему.

III. Објашњење појединих решења

Прикупљање статистичких података о свим инцидентима у ИКТ системима од посебног значаја има за циљ утврђивање стања информационе безбедности на националном нивоу. Национални ЦЕРТ ће на овај начин добити и податке о ризицима/догађајима/и свим инцидентима, не само о инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности, на националном нивоу.Наиме, оператор ИКТ система од посебног значаја дужан је да, поред обавештавања о инцидентима, достави Националном ЦЕРТ-у статистичке податке о свим инцидентима у ИКТ систему у претходној години најкасније до 28. фебруара текуће године.

Чланом 2. Правилника прописана је врста статистичких података, а кроз утврђивање јединственог обрасца који садржи податке о оператору ИКТ система од посебног значаја и о инцидентима, односно врсти и броју инцидената.

Чланом 3. Правилника утврђена је форма и начин достављања статистичких података, те предвиђено достављање електронским путем на интернет страници Националног ЦЕРТ-а.

Одредбе члана 4. Правилника односе се на поступак обједињавања статистичких података, односно на поступање и руковање овим подацима, и утврђен рок за објављивање Годишњег извештаја.

Начин објављивања дела Извештаја о статистичким податацима, који достављају оператори ИКТ система од посебног значаја, регулисан је чланом 5. Правилника, те утврђено да се појединачни делови Извештаја не могу објавити без сагласности оператора ИКТ система од посебног значаја.

Чланом 6. Правилника предвиђено је да статистички подаци достављени након законом предвиђеног рока неће бити уврштени у Годишњи извештај Националног ЦЕРТ-а.

IV. Предлог даљих активности

Предлаже се да Управни одбор Агенције размотри и усвоји Нацрт правилника, као и да исти, након тога, Агенција у складу са одредбама чл. 34-36. Закона, упути на јавне консултације у трајању од 10 радних дана.

Након спроведених јавних консултација, извршиће се обрада приспелих примедаба, предлога и сугестија и Управном одбору Агенције ће се доставити одговарајући Предлог правилника. По његовом усвајању, сагласно члану 23. став 2. ЗЕК-а и члану 57. Закона о државној управи („Службени гласник РС“, бр. 79/05, 101/07, 95/10, 47/18, 99/14, 30/18-др.закон и 47/18), овај општи акт се упућује ресорном министарству, на даљу надлежност, ради прибављања мишљења о његовој уставности и законитости. По добијеном мишљењу ресорног министарства, предметни правилник се објављује у „Службеном гласнику Републике Србије“.

V. Средства за спровођење Правилника

За спровођење овог правилника није потребно обезбедити посебна средства предвиђена финансијским планом Агенције.