РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

Упутство за пријаву инцидента

ИКТ СИСТЕМИ ОД ПОСЕБНОГ ЗНАЧАЈА У РЕПУБЛИЦИ СРБИЈИ

У ЦИЉУ **ЗАШТИТЕ** ИКТ СИСТЕМА:

- ДЕЛИТЕ ИНФОРМАЦИЈЕ И ИСКУСТВА
- ПРИПРЕМИТЕ ЗАПОСЛЕНЕ, ПРОЦЕДУРЕ И ТЕХНОЛОГИЈУ
- ПРИМЕНИТЕ **МЕРЕ ЗАШТИТЕ**
- У СЛУЧАЈУ НАПАДА

ПРИЈАВИТЕ ИНЦИДЕНТ

Инцидент је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система. Сви оператори ИКТ система од посебног значаја одговарају за безбедност ИКТ система и дужни су да у том циљу примењују мере заштите прописане Законом о информационој безбедности.

У циљу остваривања стратешког циља Владе Републике Србије- развоја и унапређења информационе безбедности у Републици Србији, Национални ЦЕРТ врши превенцију и заштиту од ризика путем размене информација, праћења актуелних ризика и подизања свести грађана, привредних субјеката и органа власти о значају информационе безбедности.

Пријављивање инцидената који могу да имају значајан утицај на нарушавање информационе безбедности предвиђена је Законом о информационој безбедности, те је операторима ИКТ система од посебног значаја прописана обавеза пријављивања инцидената. Имајући у виду да је информациона безбедност саставни део свеукупне безбедности, и да је њено очување у функцији остваривања и поштовања права, слобода и интереса грађана, привреде и државе сви друштвени чиниоци треба да буду свесни ризика повезаних са употребом технологије. Та свест се, између осталог, огледа и у ефикасној реакцији на инциденте, односно њиховом пријављивању надлежном органу.

ИКТ системи од посебног значаја су системи који се користе у обављању послова у органима јавне власти, за обраду података о личности, у обављању делатности од општег интереса у областима производње и дистрибуције електричне енергије, производња и прерада угља, истраживање, производња, прерада транспорт и дистрибуција нафте и течног гаса, промет нафте и нафтних деривата, железничког, поштанског и ваздушног саобраћаја, здравствена заштита, вођења регистра података о обавезама физичких и правних лица према финансијским институцијама, управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта, размене интернет саобраћаја, управљање регистром националног интернет домена и системом за именовање на мрежи, управљање, заштита и унапређење добара од општег интереса, као што су воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја, услуге информационог друштва, електронска комуникација, издавање службеног гласила РС, управљање нуклеарним објектима, коришћење, производња, промет и превоз наоружања и војне опреме, управљање отпадом, комуналне делатности, послови финансијских институција, услуге информационог друштва намењене другим пружаоцима услуга информационог друштва у циљу омогућавања пружања њихових услуга.

Дакле, ИКТ системи од посебног значаја су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије.

Оператори ИКТ система од посебног значаја су обавезни да о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности доставе обавештења о инцидентима:

1) који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;

2) који утичу на велики број корисника услуга;

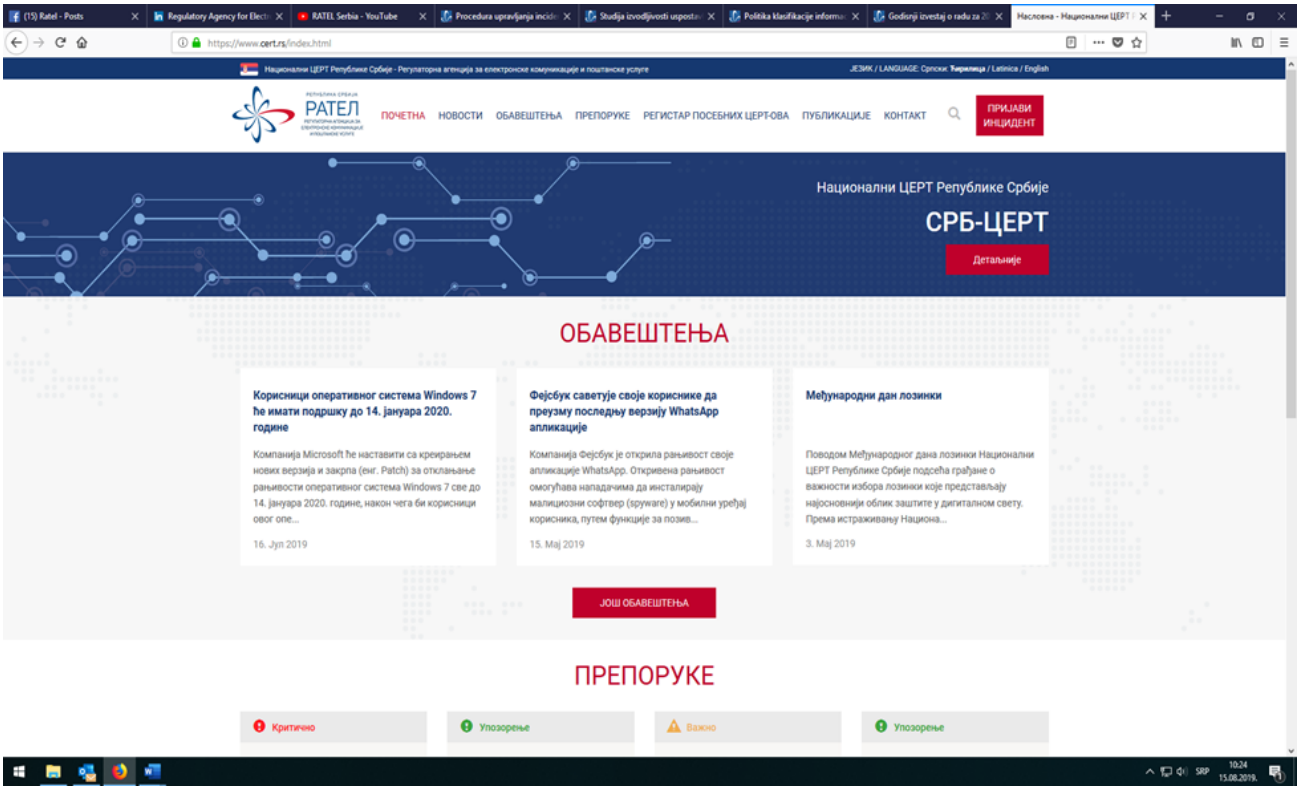
3) који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;

4) који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе.

6) који су настали као последица инцидента у ИКТ систему који се користи у пружању услуга информационог друштва, када ИКТ систем од посебног значаја користи информационе услуге ИКТ система који пружа услуге информационог друштва

Пријава инцидената врши се путем имејла на info@cert.rs, као и преко веб сајта www.cert.rs, кликом на поље „Пријави инцидент" и том приликом уносе се подаци лица које пријављује инцидент, као и подаци о инциденту, односно атрибути неопходни за даљу анализу, тип и опис инцидента.



На све мејлове примљене преко портала или имејла одговора се аутоматски. Одговор садржи линк преко кога је потребно извршити верификацију пријаве, и на тај начин потврдити пријаву инцидента. Након верификације пријаве, лицу које је пријавило инцидент доставља се потврда са идентификационим бројем и поруком да је пријава инцидента евидентирана.

Оператори ИКТ система од посебног значаја су у обавези да ове инциденте пријаве без одлагања, а најкасније наредног радног дана од дана сазнања о настанку инцидента. Препорука Националног ЦЕРТ-а је пријављивање у следећом роковима:

Опис инцидента	Рок за пријаву
Инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружања услуга	Први наредни радни дан
Инциденти који утичу на велики број корисника услуга или трају дужи временски период	Први наредни радни дан
Инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружању услуга, који утичу на обављање послова и пружање услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност	Исти дан
Инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије	Исти дан
Инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе	Исти дан
Инциденти који су настали као последица инцидента у ИКТ систему који се користи у пружању услуга информационог друштва, када ИКТ систем од посебног значаја користи информационе услуге ИКТ система који пружа услуге информационог друштва	Први наредни дан

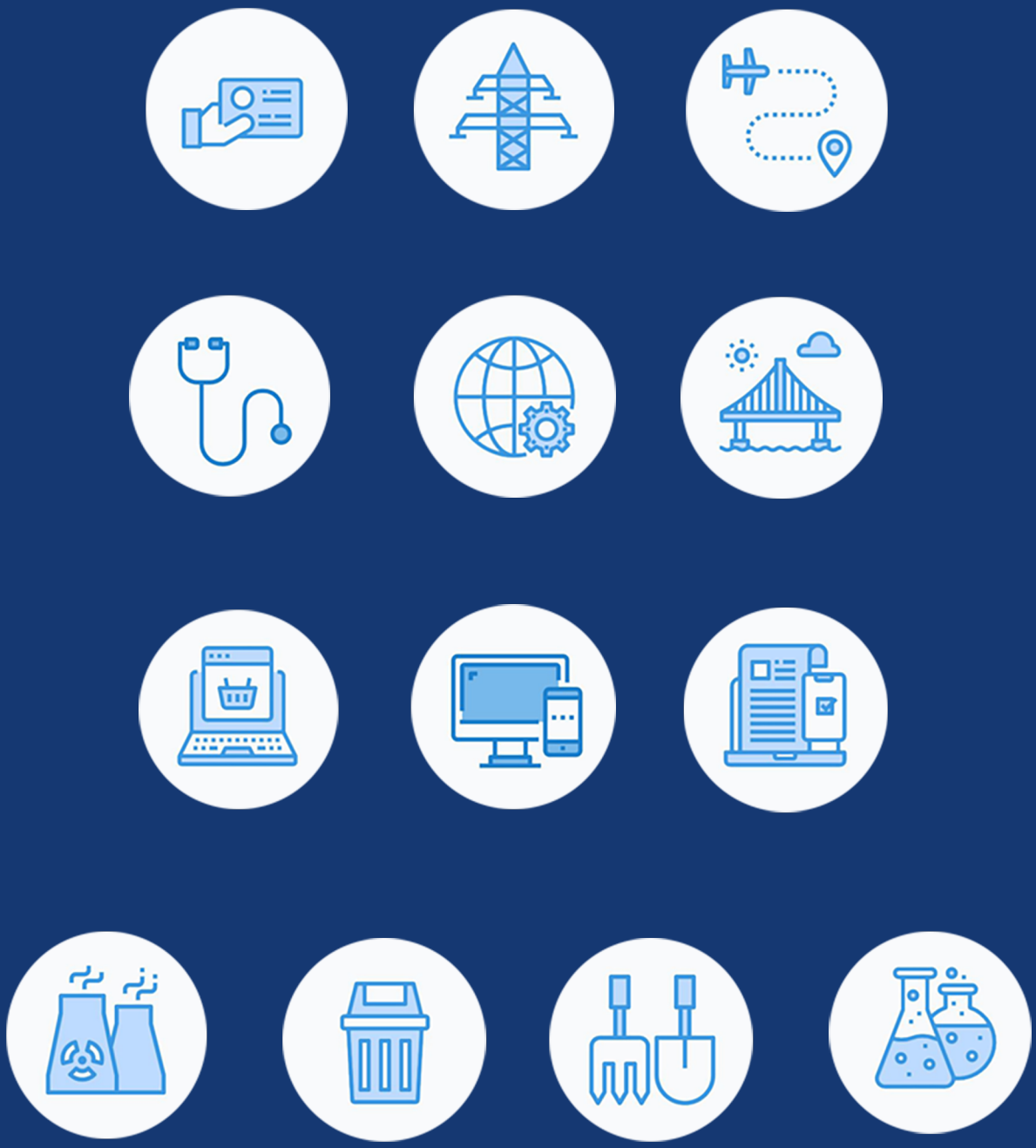
ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА		
Група инцидената	**Врста инцидента**	**Опис инцидента**
Инсталирање злонамерног софтвера у оквиру ИКТ система	Малвер (енгл. „malware")	Малвер (енг. malware) је реч изведена од две речи – "Malicious Software", и представља сваки софтвер који је написан у злонамерне сврхе, односно који има циљ да нанесе штету рачунарским системима или мрежама.
	Вирус	Рачунарски вирус је део злонамерног компјутерског кôда чији је циљ да се шири са рачунара на рачунар тако што напада извршне датотеке и документа и може проузроковати наменско брисање датотека са хард диска и сличну штету.
	Црв (енгл. „worm")	Рачунарски црв је програм који садржи злонамерни кôд који се шири преко мреже, тако што се самостално умножава и преноси, односно не зависи од датотека хоста. Црви се шире на адресе електронске поште са листе контакта жртве или искоришћавају рањивости мрежних апликација и због велике брзине ширења служе за пренос осталих типова злонамерног софтвера.
	Рансомвер (енгл. „ransomware")	Рансомвер је тип малвера, односно злонамерни софтвер који шифрира информације на уређајима или мрежама, а за приступ и откључавање датотека захтева плаћање откупа. Чест је случај да датотеке чак и након плаћања откупа остају закључане.
	Тројанац	Рачунарски тројанци (тројански коњи) су претња која покушава да се представи корисницима као да су корисни програми и на тај начин их превари да их покрену. Ови програми могу да преузму друге претње са интернета, убацују друге типове малвера на угрожене рачунаре, комуницирају са удаљеним нападачима, и бележе све што се куца на тастатури и шаљу нападачима.
	Шпијунски софтвер (енгл. „spyware")	Шпијунски софтвер делимично пресреће или преузима контролу над рачунаром без знања или дозволе корисника. Сам назив сугерише да је реч о програмима који надгледају рад корисника тако што снимају и преузимају информације са рачунара попут навика претраживања веба, електронске поште, креденцијала и сл. и те податке преносе нападачу.
	Руткит (енгл. „rootkit")	Руткит је софтвер који омогућава привилегован даљински приступ рачунару, крију̂ћи своје присуство од администратора система. Омогућава нападачу да се сакрије у току неовлашћеног приступа и одржава привилегован приступ рачунару заобилажењем уобичајеног начина аутентификације и механизама ауторизације.

ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА		
Група инцидената	**Врста инцидента**	**Опис инцидента**
Прикупљање података	Скенирање портова	Скенирање портова је напад који шаље захтеве клијената на низ адреса портова сервера хоста, са циљем откривања комуникационих канала који се могу искористити, односно проналаска отвореног порта и искоришћавања његове рањивости.
	Пресретање података између рачунара и сервера (енгл. „sniffing")	Снифер напад подразумева коришћење апликација за надгледање и анализу мрежног саобраћаја у циљу преузимања мрежних пакета. На овај начин нападач анализира мрежу и прибавља информације којим је може компромитовати.
	Социјални инжењеринг (лажно представљање и други облици)	Напади социјалног инжењеринга обично користе људску психологију и подложност манипулацијама како би навели жртве на откривање осетљивих података или кршење безбедносних мера које ће омогућити нападачу приступ мрежи.
	Повреда података (енгл. „data breaches")	Повреда података подразумева успешан злонамеран покушај који је довео до измене или губитка података.
Превара	Фишинг (енгл. „phishing")	Фишинг је сајбер напад који се врши уз помоћ електронске поште, која садржи злонамерни прилог или линк који води ка зараженом сајту или документу. Нападач користи социјални инжењеринг да би се представио као неко познат и тако навео жртву да отвори електронску пошту. Овај напад је често повезан и са нападима попут малвера, мреже ботова и сајбер шпијунаже.
	Неовлашћено коришћење ресурса (енгл. „cryptojacking" и други облици)	Криптоџекинг (познат и као криптомајнинг) односно „отимање" је нови термин који се односи на програме који користе снагу централне процесорске јединице (70% до 80% неискоришћене снаге процесора) без пристанка жртве, да би „рударили" крипто валуте за стицање личне користи.
Покушаји упада у ИКТ систем	Покушај искоришћавања рањивости система	Покушај искоришћавања рањивости система је напад на рачунарски систем, којим нападач користи одређену рањивост система. Овај напад користи рањивост оперативног система, апликације или било којег другог софтверског кода, укључујући додатке апликација или библиотеке софтвера.
	Покушај откривања креденцијала (енгл. „brute force attack")	Brute Force напад подразумева покушај приступа систему жртве непрекидним логовањем различитим комбинацијама слова, бројева и симбола са циљем идентификације корисничког имена и лозинке.

ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА		
Група инцидената	**Врста инцидента**	**Опис инцидента**
Упад у ИКТ систем	Откривање или неовлашћено коришћење привилегованих налога (енгл. „privileged account compromise")	Коришћење привилегованих налога омогућава нападачима да се непримећено крећу кроз ИКТ систем или мрежу и приступе осетљивим подацима.
	Откривање или неовлашћено коришћење непривилегованих налога (енгл. „unprivileged account compromise")	Коришћење непривилегованих налога омогућава нападачима да се непримећено крећу кроз ограничени део ИКТ система или мреже, са могућношћу даље компромитације ИКТ система или мреже и приступања осетљивим подацима.
	Неовлашћени приступ апликацији	Неовлашћени приступ апликацији је приступ веб локацији, програму, серверу, сервису или другом систему помоћу туђег налога или других метода.
	Мрежа ботова (енгл. „botnet")	Мрежа ботова је аутоматизовани напад који је скенира мрежне адресе и шири заразе на рањивим рачунарима, што омогућава хакерима да преузму контролу над зараженим рачунарима и претворе их у ботове. На тај начин се ствара мрежа ботова која се користи за нападе онемогућавања услуга (DDoS), као и за извршавање задатака без знања жртве (слање електронске поште, вируса или крађе личних података).
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. „denial-of-service attack" – DoS)	DoS напад је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.
	Вишеструки напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. „distributed denial-of-service attack" – DDoS)	DDoS је вишеструки напад који има за циљ да се поремети нормалан саобраћај сервера, услуге или мреже преплављујући инфраструктуру већом количином интернет саобраћаја. DDoS напади постижу ефикасност користећи више компромитованих рачунарских система као извора саобраћаја.
	Саботажа	Саботажа као напад се користити у сврху саботирања система или мреже и наношења штете. Могући су различити облици саботаже у зависности од области пословања нападнуте инфраструктуре.
	Прекид у функционисању система или дела система (енгл. „outage")	Прекид рада система проузрокован прекидом у испоруци електричне енергије, због лоших временских услова или хардверске грешке која је настала као последица неисправне опреме.

ЛИСТА ИНЦИДЕНАТА ПРЕМА ВРСТАМА		
Група инцидената	**Врста инцидента**	**Опис инцидента**
Угрожавање безбедности података	Неовлашћен приступ подацима	Неовлашћени приступ подацима је напад помоћу ког се кршењем мера заштите приступа подацима система или мреже у циљу њихове злоупотребе.
	Неовлашћена измена података	Неовлашћена измена података је напад помоћу ког се кршењем мера заштите приступа подацима система или мреже и врши њихова измена, а у циљу њихове злоупотребе.
	Криптографски напад	Криптографски напад је метод заобилажења мера заштите криптографског система проналажењем слабости у коду, шифри, алгоритму, криптографском протоколу или шеми управљања кључевима. Овај процес се такође назива «криптоанализа".
Остали инциденти	Инциденти који не спадају у горе наведене категорије	

Захваљујући оствареној међународној сарадњи са другим националним ЦЕРТ-овима, као и чланству у међународним организацијама Национални ЦЕРТ је поуздани координатор информација о инцидентима и посебно указује на значај пријављивања инцидената.



www.cert.rs