# ГОДИШНА ПРОГРАМА НА НАЦИОНАЛНИОТ ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ ЗА 2017 ГОДИНА

**Агенција за електронски комуникации**

Содржина:

## КРАТЕНКИ

| | |
|---|---|
| сајбер простор | информациските системи и услуги директно или индиректно поврзани на Интернет, телекомуникациските и компјутерските мрежи, електронските комуникациски мрежи |
| CIRT | Computer (Cyber) Incident Response Team (тим за справување со компјутерски инциденти)<br>Други кратенки со слично значење:<br>CSIRT - Computer Security Incident Response Team<br>CSRC - Computer Security Response Team<br>CIRC - Computer Incident Response Center<br>CERT - Computer Emergency Response Team<br>IHT - Incident Handling Team<br>IRC - Incident Response Center,<br>IRT - Incident Response Team |
| MKD-CIRT | Национален центар за одгвоор на компјутерски инциденти<br>https://mkd-cirt.mk |
| АЕК | Агенција за Електронски Комуникации<br>http://www.aec.mk |
| MARnet | Macedonian Academic Research Network (Македонска истражувачка Национална мрежа)<br>http://marnet.mk |
| ITU | International Telecommunication Union<br>http://www.itu.int/en/Pages/default.aspx |
| Национален/Владин CIRT | е тим кој и служи на Владата на начин што и помага да ги заштити клучните/критичните информациски инфраструктури во државата. Националниот/Владин CIRT има клучна улога при координација на справувањето со инциденти кај засегнатите субјекти на национално ниво. Национален/Владин CIRT преставува официјална национална точка за контакт за размена на информации и соработка со Националните/Владини CIRT-ови од другите држави (според дефиниција на ENISA) |
| ENISA | European union Agency for Network and Information Security<br>https://www.enisa.europa.eu/ |
| FIRST | Forum for Incident Response and Security Teams<br>https://www.first.org/ |
| TF-CSIRT | Trusted Introducer<br>https://www.trusted-introducer.org/ |

| | |
|---|---|
| CERT-EU | Computer Emergency Response Team for EU institutions<br>https://cert.europa.eu/cert/plainedition/en/cert_about.html |

## ПРАВЕН ОСНОВ ЗА ДОНЕСУВАЊЕ НА ГОДИШНАТА ПРОГРАМА

Врз основа на член 26-а став 2 и 3 од Законот за електронските комуникации (Службен весник на Република Македонија број 39/2014, 188/2014, 44/2015 и 193/2015) , Директорот на Агенцијата за електронски комуникации во соработка со министерот надлежен за работите од областа на електронските комуникации донесува Годишна програма за работењето на националниот центар за одговор на компјутерски инциденти формиран како посебна организациона единица во состав на Агенцијата за електронски комуникации и истата ја доставува на усвојување од страна на Владата на Република Македонија.

## ВОВЕД

Сигурен и безбеден сајбер-простор, односно сигурни и безбедни информациски системи и мрежи од компјутерски напади и инциденти обезбедува политичка и општествена вклученост; намалување на бариерите помеѓу државите, заедниците и граѓаните; овозможување интеракција и размена на идеи и информации; обезбедување слобода на изразување и слобода на медиумите; практикување на фундаменталните права и обезбедување можност граѓаните да развиваат подемократско општество.
Сеуште добар дел од граѓани немаат доверба во користењето на интернетот за услугите на електронско трговија и банкарство, поради нивната загриженост за безбедноста на податоците и можноста од нивна злоупореба. Се забележува и тренд на континуирано зголемување на јавни објави за упади во кориснички сметки и пораст на уцени преку ransomware малициозни софтвери како вектори за извршување на сајбер напади. Дополнително и Internet of things ја зголемува површината за сајбер напади.

Сајбер-просторот не е целосно регулиран со што е овозможено компјутерскиот криминал да биде едноставен и евтин за извршување.

Компјутерските/сајбер напади, врз информациските системи и мрежите мотивирани од криминални побуди стануваат се поголема глобална закана.

Со измените на Законот за електронските комуникации (Службен весник на Република Македонија број 188/2014), согласно член 26-а во состав на Агенцијата за електронски комуникации се формира посебна организациона единица - Национален центар за одговор на компјутерски инциденти MKD-CIRT, која ќе претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој ќе идентификува и ќе обезбедува одговор на безбедносни инциденти и ризици.

## МИСИЈА

Националниот центар за одговор на компутерски инциденти ја има следната мисија:

a) да координира и да помага/асистира на органите и институциите од јавниот сектор во имплементацијата на проактивните услуги за намалување на ризикот од компјутерски безбедносни инциденти, како и при справувањето со инцидентите кога истите ќе настанат ,
b) да спроведува активности за едуцирање и подигање на свесноста кај граѓаните за негативните ефекти на сајбер заканите и компјутерскиот криминал, и
c) навремено да обезбедува совети за сите негови конституенти.

## КОНСТИТУЕНТИ

Конституенти од јавниот сектор и претставници на критична инфраструктура во Република Македонија со кои MKD-CIRT ќе соработува во реализацијата на програмата за работа за 2017 година ќе вклучи организации од следните сектори: јавен сектор, финансии, комуникации, енергетика, водоснабдување, итни услуги, храна, јавна безбедност, здравство и услуги на е-влада. Во 2017 година ќе се продолжи со активностите за размена на информации со постојните и нови организации како кнституенти на MKD-CIRT, како и потпишување на поодделни договори за соработка и одгвоорно откривање на информации. Следува листа на организации со кои MKD-CIRT во 2016 година воспостави мрежа за безбедна размена на информации, за чии претставници организираше обуки и работилници и со кои ќе продолжи да соработува во 2017 година.

Генерален секретеријат на Владата на Република Македонија

Кабинет на премиерот на Република Македонија

Министерство на информатичко општество и администрација

Министерство на одбрана

Министерство за внатрешни работи

Министерство за финансии

Агенција за разузнавање

Дирекција за заштита на лични податоци

Дирекција за безбедност на класифицирани информации

Македонска академска истражувачка мрежа (МарНет)

Центар за управување со кризи

МЕПСО

ЕВН

Народна банка на Република Македонија

Стопанска банка

Комерцијална банка

Македонски Телеком

## ЦЕЛИ И ЗАДАЧИ

Основните цели и задачи на националниот центар за одговор на компјутерски инциденти MKD-CIRT се :

Ц1. Да обезбеди клучна улога при координација на справувањето со инциденти кај засегнатите субјекти на национално ниво.

Ц2. Да обезбеди одговор за справување со компјутерски инциденти, преку давање на неопходни услуги кон неговиот конституент/корисник, со што неговиот конституент/корисник ќе може ефикасно да се справи со инцидентите.

Ц3. Континуирано да врши мониторингот за ризици, да добива информации за компјутерските закани и инциденти (по автоматски пат или од трети страни) и постојано да располага со показатели за малициозниот сообраќај што доаѓа или излегува од државата.

Ц4. Преставува официјална национална точка за контакт и размена на информации (извештаи за инциденти, ранливост итн.) за внатре во рамките на државата како и за надвор од неа со Националните/Владини CIRT-ови од државите во регионот и пошироко.

Ц5. Да навремено ги информира и известува конституентите. Да им обезбедува на конституентите безбедносни совети, информации за рано предупредување и да делува како централна точка за прашањата од областа на сајбер безбедноста.

Ц6. Целосно да соработува и разменува информации со институциите од државата надлежни за спроведување на законите, а особено со оние од областа на сајбер криминалот, како исоодветно да ги адресира правните прашања кои можат да се појават за време на инцидент.

Ц7. Континуирано да разменува информации, знаење и искуство со конституентите, да утврдува безбедносни најдобри практики/водичи и истите да ги објавува, како и континуирано да обезбедува едукација и обуки за конституентите и за самите вработени во центарот.

Ц8. Да обезбедува помош во процесот на воспоставување на Интерни центри за одговор на компутерски инциденти на големите организации кои управуваат со клучни/критични информациски инфраструктури (јавни и приватни) во Република Македонија.

Ц9. Континуирано да ја подига свесноста кај граѓаните за негативните ефекти на сајбер заканите и компјутерскиот криминал

### (Ц1) Обезбеди клучна улога при координација на справувањето со инциденти кај засегнатите субјекти на национално ниво.

При пријава или идентификација на компјутерски инцидент, центарот за одговор на компјутерски инциденти ќе обезбеди клучна улога при координирање на активностите кои ќе бидат потребни да се спроведат за справување со компјутерскиот инцидент. Координацијата се однесува на вклучување и известување на засегнати субјекти на

национално ниво, за решавање и надминување на пријавениот компјутерски безбедносен инцидент.

За исполнување на оваа цел во 2017 година ќе се реализираат следните активности:

- навремено ќе се ажурира регистар на контакти со конституенти за справување со кризна состојба и инциденти;
- ќе се обезбеди достапност на различни безбедносни канални за комуникација со соодветните субјекти на национално ниво;
- ќе се подготвуваат соодветни упатства и процедури за надминување на стандардни и познати компјутерски инциденти и безбедносни закани;
- MKD-CIRT ќе ја анализира потребата од доставување на предлог за измена на Законот за електронските комуникации
- предлози за изработка на нови и измена на постојни правилници и други подзаконски акти;

## (Ц2) Обезбедување на одговор за справување со компјутерски инциденти, преку давање на неопходни услуги кон неговиот конституент/корисник, со што неговиот конституент/корисник ќе може ефикасно да се справи со инцидентите.

Согласно усвоените препораки во извештајот на ITU-IMPACT, услугите кои MKD-CIRT ќе ги пружа на конституентите и граѓаните на Република Македонија се поделени во три групи: основни, подобрени и напредни услуги. Предуслов за успешно пружање на овие реактивни и проактивни услуги е квалитетно и целосно екипирање на тимот на MKD-CIRT. Услугите од групата „напредни услуги“ ќе бидат достапни за конституентите во втората половина на 2017 година.

| | Основни услуги (Basic services) | Опис |
|---|---|---|
| 1 | Известувања и предупредувања | Откривање на детали за тековните закани и чекори кои можат да се преземат за заштита од овие закани. Вклучува известување или предупредување за новооткриената информација за сајбер закани и слабости до конституентите со препорачан тек на акции и насоки за тоа како да се заштити системот. Известувањата може да се превентивни, предупредувачки, советодавни, и насочувачки. |
| 2 | Далечински одговор на инцидент | Обезбедување на техничка помош за справување со безбедносните инциденти кога ќе се појават, со цел ублажување на штетата и опоравување од инцидентот. Советите и техничката помош вообичаено ќе се обезбедуваат преку телефон или e-mail-базирана комуникација |
| 3 | Одговор на инцидент на лице место | Обезбедување на техничка поддршка и совети за справување со безбедносните инциденти кога ќе се појават на лице место кај конституентот, со цели ублажување на штетата и опоравување од инцидентот. Оваа услуга вообичаено е поврзана и се реализира при инциденти од критично ниво. |
| 4 | Одговор на ранливост | Оценување на соодветни мерки потребни за да се одговори на новооткриени слабости; да се оцени нивната сериозност и влијание, да се одлучи дали да издадат предупредувања за нив или да се потврдат или понатаму да се испита нивната тежина / влијание. Генерално, овој пристап се однесува на информации за ранливости кои се веќе јавно познати. |

| | | |
|---|---|---|
| 5 | Основна свест, едукација и обука | Спроведување на програми од мали размери за подигнување на јавната свест. Спроведување на основни обуки за одговор на компјутерски инциденти и основни сајбер безбедносни најдобри практики. |

| | Подобрени услуги (enhanced services) | Опис |
|---|---|---|
| 1 | Координација на одговор на инцидент | Дејствување како координативна точка на национално или регионално ниво помеѓу страните засегнати од безбедносниот инцидент. За да може да ја обезбеди оваа услуга, MKD-CIRT мора да воспостави доверлива комуникација со различни страни и агенции на национално, регионално и глобално ниво. |
| 2 | Напредна свест, едукација и обука | Спроведување на програми од широки размери за подигање на јавната свест како на пр. конференции на национално или регионално ниво. Спроведување на напредни обуки за одговор на компјутерски нциденти и напредни сајбер безбедносни најдобри практики. |
| 3 | Координација на одговор на ранливост | Координација на одговорно објавување на информации во врска со софтверски/хардверски ранливост во соодветен временски период. Времето на објава се одредува на тој начин за да се минимизираат негативните последици од предвремено откривање, преку обезбедување на доволно време за добавувачот да развие и објави закрпа и тоа време да се совпадне со известувањето. |
| 4 | Анализа на закани и ранливости | Анализата на компјутерски и мрежни закани и ранливости со цел да се одреди нивното можно/потенцијално влијание и како најдобро истите да се ублажат; Идентификација на новите трендови или промени во начинот на работење на напаѓачот; или советување во врска со општите трендови во сајбер безбедноста. |

| | Напредни услуги (Advanced services) | Опис |
|---|---|---|
| 1 | Форензичка анализа | Спроведување на дигитални форензички анализи на дигитални докази и артефакти во согласност со законите во Република Македонија. Тоа е реактивен услуга со која членовите на тимот на MKD-CIRT ќе реагираат и одговорат на инцидентот за испитување и устврдување на штета и |

| | | |
|---|---|---|
| | | евентуално идентификаиција на сторителот. |
| 2 | Безбедносна проценка и ревизија | Консултантски услуги за да обезбеди извештај за процена на безбедноста на информатичките системи / мрежи на Конституентот; истакнување на сите слабости и предлагање на методи за да се подобри безбедноста.<br>Вид на услуги:<br>- анализа на ризик<br>- деловен континуитет и Disaster Recovery планирање<br>- безбедносни консултации<br>- Евалуација или сертификација на производи. |

За реализација на услугите на MKD-CIRT неопходно е екипирање на тимот со квалитетен кадар, набавка на соодветна опрема за оцена на ранливост на системите и мрежите кај конституентите, набавка на опрема за форензичка анализа по настанат инцидент кај конституент и обука на вработените во тимот за користење на опремата. Услугите на MKD-CIRT кои се однесуваат на справување со пријавен инцидент кај конституент ќе побаруваат потпишување на соодветни договори со кои ќе се дефинира опсегот на системите и мрежите кои ќе бидат предмет на анализа и истражување по пријавениот инцидент како и за предложени и прифатени мерки за ублажување на влијанието на инцидентот и опоравување на мрежите и системите на конституентот. .

(Ц3) Континуирано да врши мониторингот за ризици, да добива информации за компјутерските закани и инциденти (по автоматски пат или од трети страни) и постојано да располага со показатели за малициозниот сообраќај што доаѓа или излегува од државата.

Континуираното мониторирање на компјутерските закани и инциденти ќе биде реализирано со:

- користење на соодветни софтверски решенија за нивна евиденција
- пратење на содржини презентирани на интернет во доменот за сајбер безбедност и малициозен сообраќај
- пратење и учество во форуми на интернет како привилегија обезбедена преку членство во меѓународни организации
- овозможување на локална дојава и информации за идентификирана компјутерска закана или инцидент.

За исполнување на оваа цел MKD-CIRT во 2017 година ќе ги преземе следните активности:

- воспоставување на систем за прибирање, обработка, корелација и дисеминација на информации за ранливости (threats intelligence system)
- Договори за соработка и раземна на информации со производители/вендори на оперативни системи и решенија за информациска безбедност, преку кои ќе се обезбедни пристап до инофмрации за т.н. zero-day ранливости и упатства за нивно ублажување кои потоа MKD-CIRT ќе ги испраќа до конституентите.
- Анализа на ранливости на јавните веб локации на конституентите и организациите од јавниот сектор и Проект за процена на состојба со информациска безбедност на јавниот веб простор во Македонија за што е неопходна набавка на соодветна опрема и поставување на систем за откривање на ранливости Како резултат од анализата MKD-CIRT ќе достави доверливи извештаи за најдени ранливости за секој конституент одделно и ќе објави анонимизиран кумулативен јавен документ за ранливоста на јавните веб седишта на организациите од јавниот сектор, со што ќе се добие реална слика за нивото на имплементирани тех нички мерки за заштита.

(Ц4) Преставува официјална национална точка за контакт и размена на информации (извештаи за инциденти, ранливост итн.) за внатре во рамките на државата како и за надвор од неа со националните/владини CIRT-ови од државите во регионот и пошироко.

Исполнувањето на оваа цел ќе се реализира со иницирање на зачленување или пристапување на Република Македонија и MKD-CIRT во меѓународни организации:

- Пристапување на Република Македонија и MKD-CIRT како официјална национална точка за контакт и координација на одговор на компјутерски инциденти кон иницијативата ITU CIRT Programme. Оваа инцијатива организирана од страна на ITU (International Telecommunications Union) поврзува национални CIRT тимови од над 100 земји во светот и за основна цел има јакнење на капацитетите на националните тимови. Услугите кои ги нуди се поделени во три фази: процена, имплементација и сајбер вежби. MKD-CIRT ќе соработува со ITU и оваа програма во делот на имплементација и сајбер вежби.
- Информирање на ENISA за воспоставувањето на MKD-CIRT како национална точка за размена на информации за Република Македонија. Европската Агенција за мрежна и информациска безбедност заедно со CERT-EU се централна точка за координација и размена на информации меѓу националните CIRT тимови во земјите членки на Европската Унија.
    - Информирање на националните CIRT тимови во земјите членки на Европската Унија за воспоставување на MKD-CIRT како официјална национална точка за размена на информации и координација на меѓународни активности со Република Македонија.
    - Иницирање на спремност за соработка во припрема и реализација на сајбер безбедносни вежби преку кои ќе се јакнат капацитетите на MKD-CIRT и конституентите, а истовремено ќе се овозможи зголемена меѓународна афирмација на MKD-CIRT
    - Иницирање на барање за пристап до ресурсите кои ENISA ги обезбедува на другите национани CIRT-ови, како известувања, најдобри практики и работни групи.
- зачленување во FIRST. FIRST како форум на CIRT тимови нуди помош во комуникацијата меѓу одделни CIRT-ови преку нивно запознавање или преку

користење на воспоставената инфраструктура и системи за споделување на информации и соработка. Оваа соработка има основна цел да го забрза процесот на справување со компјутерските безбедносни инциденти.

- зачленување и акредитација на MKD-CIRT во TF-CSIRT Trusted Introducer како меѓународна организација која нуди услуги на CIRT-тимови. Со зачленувањето на MKD-CIRT ќе се постигне:
  - MKD-CIRT да биде запишан во евиденцијата и листата на CIRT тимови како официјална национална точка за контакт во Република Македонија, со што CIRT тимовите што членуваат во TF-CSIRT ќе бидат информирани за воспоставувањето на MKD-CIRT;
  - Пристап до ресурсите, инфраструктурата и системите на TF-CSIRT;
  - Акредитација на MKD-CIRT како CIRT тим со воспоставени најдобри практики и имплементирани политики од Trusted Introducer во своето работење со што MKD-CIRT би се здобил со повисоко ниво на доверба во комуникацијата со останатите членови.
- Пристапување кон програмата за развој на национални тимови CSIRT development Program на CERT при Software Engineering Institute, Carnegie Mellon University, преку која се нуди помош за воспоставување на национални тимови, организација на работењето во тимот, прибирање на докази/форензика, управување со инциденти и објава на информации
- Продолжена и засилена активност за соработка со национални и владини CIRT тимови од земјите во регионот. Активноста е отпочната во 2016 година и во 2017 година цел е да се иницира соработка со тимови од други земји со можност за нејзино официјализирање преку потпишување на меморандуми за соработка во делот на:
  - Размена на информации за безбедна и доверлива комуникација;
  - Размена на информации, известувања и аалрмирање за безбедносни ранливости и инциденти;
  - Соработка, координација и заемна помош во справување со меѓународни безбедносни инциденти;
  - Учество на локални експери од MKD-CIRT и конституентите во регионални работилници и вежби за сајбер безбедност;
  - Организација на регионална конференција на национални и секториски CIRT-ови од регионот на југоисточна Европа. Конференцијата има за цел да

се разменат искуства со 10-тина тимови од регионот, потпишување на меморандуми за билатерална и мултилатерална соработка во делот на споделување на информации и координација на активностите во справување со компјутерски безбедносни инциденти. Конференцијата ќе има и едукативна компонента, со предавања од експерти од тимовите со цел едукација и јакнење на капацитетите на тимовите-учесници на конференцијата. Конференцијата ќе биде дел од Меѓународната регулаторна конференција што Агенцијата за електронски комуникации ќе ја оргаизира во 2017 година.

- Информирање на јавноста во Република Македонија за MKD-CIRT како официјална национална точка за координација и размена на информации преку испраќање на соопштенија до медиумите и континуирано информирање на јавноста за безбедносните закани и начини за заштита.
- Информирање на конституентите и организациите од јавниот и приватниот сектор за MKD-CIRT и неговите услуги преку презентации на услугите и активностите на MKD-CIRT на јавни состаноци, состаноци со здруженија и испраќање на соопштенија и информации за начинот на пружање на услугите и за начинот на воспоставување на соработка.

### (Ц5) Конституентите навремено да ги информира, известува, да им обезбедува безбедносни совети, информации за рано предупредување и да делува како централна точка за прашањата од областа на сајбер безбедноста.

Конституентите времено ќе бидат информирани со обезбедување на комуникација преку безбедносни канали и тоа :

- континуирана достапност, подобрување и надградба на платформите за комуникација со констинуентите и граѓаните со MKD-CIRT (телефон, е-маил, факс, писмен допис, web итн).
  - веб страниците наменети за совети, рано предупредување како и за општи информации од областа на сајбер безбедноста
  - PGP-енкриптирана емаил комуникација
  - Поставување на систем за дисеминација на информации до конституентите

- освен традиционалните комуникациски канали, дисеминацијата на помалку критични или помалку чуствителни (пред се јавни) информации кон своите конституенти и јавноста преку нови платформи (Facebook, Twitter, mailing lists, RSS feeds)., со цел подигнување на јавната свест за сајбер безбедноста

### (Ц6) Целосно соработува и разменува информации со институциите од државата надлежни за спроведување на законите, а особено со оние од областа на сајбер криминалот

Националиот центар за одговор на компјутерски инциденти целосно ќе биде посветен за соработка и размена на информации со останатите државни институции кои се надлежни за спроведување на законската рамка на Република Македонија за технички и организациски мерки за обезбедување на тајност и заштита на обработка на податоци, безбедност на мрежи,заштита на лични податоци како и од областа на сајбер криминалот.

Во текот на овој период центарот ќе предложи предлог промени во Законот за електронски комуникации со цел подетално дефинирање на конституентите, обврските на MKD-CIRT, начинот и временските рамки за пријава на инциденти од страна на конституентите како и промени во Правилникот за обезбедување на безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и активности кои што операторите треба да ги преземат при нарушување на безбедноста на личните податоци, за поефикасно координирање на активностите за справување со компјутерските безбедносни инциденти и за обезбедување проток на информации за безбедноста и интегритетот на сите комуникациски мрежи. Дополнително ќе се направи и анализа за потребата од измени на законот и подзаконските акти со цел усогласување со европската директива за безбедност на мрежи и информациски системи донесена во 2016 година - The Directive on security of network and information systems (NIS Directive). Резултатите од анализата ќе се искористат за предлози за измена на законската рамка во Република Македонија.

## (Ц7) Континуирано да разменува информации, знаење и искуства со конституентите, да утврдува безбедносни најдобри практики/упатства

Важна компонента во функционирањето на центарот е обезбедување на кадар кои ќе може технички да одговори на сите предизвици за одговор на компјутерски инциденти.

Сведоци сме на зголемениот премин на малициозниот софтвер во сферата на платени услуги со цел уцена на сопствениците на информациите. За пратење на овој брз тренд на развој на нови компјутерски закани и нивната се покомплексна структура и дистрибуција, едукацијата и надградбата на вработените во центарот се од извонредно значење.

Едукација на вработените ќе биде преку самоедукација со користење на едукативни материјали достапни на интернет, преку посета на специјалнизирани курсеви за CIRT тимови организирани од меѓународни организации ( пр. TERENA/GEANT TRANSIT I, TRANSIT II и др.) но и со размена на искуства со локалните, регионалните и меѓународните центри за одговор на компутерски инциденти преку работилници и семинари.

MKD-CIRT во 2017 година континуирано ќе разменува информации, знаење и искуство со конституентите, ќе утврдува безбедносни најдобри практики/водичи и истите ќе ги објавува. Во таа насока, MKD-CIRT континуирано ќе обезбедува едукација и обуки за вработените и за конституентите.

Едукацијата на вработените е во насока на здобивање со знаења и вештини во делот на информацискатa безбедност, управување со информациска безбедност, управување со процес за справување со компјутерски безбедносни инциденти, penetration testing, откривање и анализа на ранливости и форензика по настанат инцидент. Потврда на стекнатите знаења ќе се врши преку сертификација на вработените согласно меѓународно признаените сертификации од страна на ENISA, ITU и EU, во делот на:

- Управување со информациска безбедност и Управување со процесите за справување со безбедносни инциденти, како на пример ISC2 CISSP (Certified Information Security Professional), ISACA CISM (Certified Information Security Manager), EC Council CCSO (Certified Chief Information Security Officer), EC Council CIH (Certified Incident Handler)
- Форензика, Penetration testing и енкрипција, како на пример EC Council CES/CEH/CHFI (Certified Encryption Specialist/Certified Ethical Hacker/Computer Hacking Forensics Investigator)

- Анализа и управување со ризици како на пример ISACA CRISC (Certified in Risk and Information System Control) и ISO 27005 (Risk Management)

Едукација на конституентите е во насока на јакнење на капацитетите на лицата и тимовите задолжени за информацискатa безбедност на страна на конституентите. За исполнување на оваа цел MKD-CIRT во 2017 година ќе организира работилници за конституентите. Поделатен опис на работилниците е даден во активностите за исполнување на следната цел – Ц8.

Во 2017 година MKD-CIRT ќе објавува информации, упатства и најдобри практики наменети за конститунетите во делот на процена на ризик, процена на ранливости на системите и мрежите на конституентите и упатства за ублажување на ефектите од актуелни сајбер закани и за надминување на откриени ранливости.

## (Ц8) Обезбедува помош во процесот на воспоставување на интерни центри за одговор на компјутерски инциденти на големите организации кои управуваат со клучни/критични информациски инфраструктури (јавни и приватни) во Република Македонија

Една од поважните активности на националниот центар за одговор на компјутерски инциденти е иницирање на воспоставување на интерни центри за одговор на компјутерски инциденти , особено на организации кои управуваат со клучни/критични информациски инфраструктури, и на барање од конституентите учество и давање на помош во самиот процес на воспоставување на интерни центри за одговор на компутерски инциденти, особено на организации кои управуваат со клучни/критични информациски инфраструктури.

Ова е од големо значење заради повеќе причини и тоа :

- Зголемување на бројот на обучен технички персонал одговорен за одговор на компјутерски инциденти
- Подобрување на одржувањето и превентивно делување на ниво на институција за обезбедување на заштита против компјутерски инциденти
- Обезбедување на брза и ефикасна реакција при кризни ситуации
- Подигање на нивото на свест за сајбер безбедност на поединечни институции

За исполнување на оваа цел во 2017 година MKD-CIRT ќе ги преземе следните активности:

- Организирање на работилници за конституентите на теми:
  - Управување со процесот за справување со инциденти
  - Методи за самостојна процена на ранливоста на информациските системи и мрежи и процена на ризиците во организациите на конституентите
  - Имплементација на најдобри пракси за техички и организациски мерки за безбедност на мрежи и системи

## (Ц9) Подигање на свесноста кај граѓаните за негативните ефекти на сајбер заканите и компјутерскиот криминал

Важна превентивна мерка за борба против компјутерските инциденти и компјутерскиот криминал е подигањето на свесноста на граѓаните за сајбер безбедноста.
Оваа цел ќе се остварува со овозможување на услугата за едукација и обука.

Во 2017 година се планираат следните активности за да се задоволат овие цели:

- Испитување на јавно мислење со цел да се добие слика за информираноста на граѓаните за сајбер заканите и користењето на интернет услуги
- Објава на основни едукативни содржини за сајбер безбедност на официјалната страница на центарот https://mkd-cirt.mk
- Објава и промоција на интерактивни едукативни содржини за веб, мобилни и социјални платформи за сајбер безбедност како континуирана активност
- Објава на содржини за различни групи на граѓани по години на старост за презентирање преку разни информациски канали и платформи (веб, twitter, facebook).
- Јавни кампањи за безбедност на интернет за подигање на свеста на граѓаните за заштите од сајбер напади преку социјалните мрежи и традиционалните информативни медиуми (Октомври – месец на сајбер безбедност)

## АКЦИСКИ ПЛАН

Акцискиот план за 2017 година на националниот центар за одговор на компјутерски инциденти MKD-CIRT е прикажан во табелата 1. За секоја активност е наведен период на реализација.

**Табела 1**

| Ред.бр. | Активност | Временска рамка<br>(Q – Квартал) |
|---|---|---|
| 1 | Одржување и надградба на систем за пријава, евиденција и управување со компјутерски безбедносни инциденти. | Q1-Q4 |
| 2 | Поставување на систем за управување со квалитет на услуги за следење на ефикасноста на центарот за одговор на компјутерски инциденти и обезбедување на постојан процес на негово подобрување . | Q1-Q4 |
| 3 | Контнуирана активност за обезбедување безбеден начин на пријавување на инцидентите преку различни канали за комуникација : телефон/мобилен, е-маил со PGP енкрипција, факс, писмен допис, и web формулари . | Q1-Q4 |
| 4 | Одржување, објава на информации, упатства и најдобри практики како и надградба на официјалниот веб сајт достапен на адреса https://mkd-cirt.mk со следните функционалности<br>○ Општи информации за центарот<br>○ Овозможување на пријава на инцидент и нелагелана содржина<br>○ Известувања за тековните информации за безбедносни инциденти<br>○ Пристап до документација ( годишните извештаи, ...)<br>○ Листа на сервиси и нивно иницирање<br>○ Настани<br>○ Линкови до корисни информации и веб страници | Q1-Q4 |

| | | |
|---|---|---|
| | ○ Законска регулатива<br>○ Контакти<br>○ Јавен дел за објава на информации, известувања и совети кои имаат за цел подигнување на јавната свест за сајбер безбедноста и сајбер заканите<br>○ Заштитен дел за безбедна комуникација со конституентите | |
| 5 | Припрема на нови и ажурирање на постојни упатства и процедури за:<br>○ Обработка на пријави од страна на<br>○ надворешни центри<br>○ конституентите<br>○ Граѓани<br>○ Сервиси према конституентите<br>○ Начин на однесување и проток на информации (code of conduct)<br>○ Класификација на компјутерските безбедносни инциденит<br>○ Обработка и постапување по класифицираните инциденти | Q1-Q4 |
| 6 | Информирање на јавноста на Република Македонија и објавување на основни едукативни содржини за сајбер безбедност на официјалната страница на центарот | Q1-Q4 |
| 7 | Припрема на содржини за различни групи на граѓани по години на старост за презентирање преку медиумски канали | Q3-Q4 |
| 8 | Информирање на конституентите и собирање на податоци за нивната инфраструктура ,овластените контакти и јавни PGP клучеви за безбедна комуникација и размена на информации | Q1-Q4 |
| 9 | Добивање на безбедносни сертификати за вработените | Q1-Q4 |
| 10 | Пристапување во меѓународните организации како официјална национална точка за контакт за одговор на компутерски инциденти. | Q1-Q4 |
| 11 | Воспоставување на систем за прибирање, обработка, корелација и дисеминација на информации за ранливости (threats intelligence | Q3 |

| | | |
|---|---|---|
| | system) | |
| 12 | Договори за соработка и размена на информации со производители/вендори на оперативни системи и решенија за информациска безбедност, преку кои ќе се обезбеди пристап до информации за т.н. zero-day ранливости и изработка на упатства за нивно ублажување кои потоа MKD-CIRT ќе ги испраќа до конституентите. | Q1-Q4 |
| 13 | Анализа на ранливости на јавните веб локации на конституентите и организациите од јавниот сектор и Проект за процена на состојба со информациска безбедност на јавниот веб простор во Македонија за што е неопходна набавка на соодветна опрема и поставување на систем за откривање на ранливости | Q3-Q4 |
| 14 | Организација на регионална конференција на национални и секториски CIRT-ови од регионот на југоисточна Европа. | Q2 |
| 15 | Поставување на систем за дисеминација на информации до конституентите | Q2-Q3 |
| 16 | Организирање на работилници за конституентите | Q2, Q4 |
| 17 | Испитување на јавно мислење | Q2, Q4 |
| 18 | Јавни кампањи за безбедност на интернет | Q4 |

# ОРГАНИЗАЦИЈА

## Организација и расположиви ресурси

Националниот центар за одговор на компјутерски инциденти е формиран како посебна организациона единица во состав на Агенцијата за електронски комуникации.

Извадок од органограмот на внатрешна организација на АЕК е претставен на слика 1.

**Слика 1**

## Човечки ресурси

За националниот центар за одговор на компјутерски инциденти планирани се 5 работни места со структура претставена во табела 2.

**Табела** 2

| Работно место во систематизација | Стручна спрема | Шифра на работно место | | | | |
|---|---|---|---|---|---|---|
| Раководител на Служба-Национален центар за одговор на компјутерски инциденти | ВСС | АЕК | 01 | 01 | Б02 | 1 |
| Советник за одговор на компјутерски инциденти | ВСС | АЕК | 01 | 01 | В01 | 1 |
| Советник за одговор на компјутерски инциденти | ВСС | АЕК | 01 | 01 | В01 | 1 |
| Советник за одговор на компјутерски инциденти | ВСС | АЕК | 01 | 01 | В01 | 1 |
| Советник за одговор на компјутерски инциденти | ВСС | АЕК | 01 | 01 | В01 | 1 |

Вработените во MKD-CIRT здолжително мора да поседуваат безбедносни сертификати за пристап до класифицирани информации издадени од Дирекцијата за безбедностг на класифицирани информации согласно член 38 од Законот за класифицирани информации и согласно меѓународните препораки (ITU, ENISA,EU). Вработените во MKD-CIRT треба да поседуваат овластувања за обработка на лични податоци издадени од Агенцијата за електронски комуникации.

Кандидатите за работа во MKD-CIRT задолжително треба да поседуваат сертификат кој има поврзаност со информациска и комуникациска безбедност , додека предност ќе имаат кандидатите кои поседуваат меѓународно признаени сертификати од страна на ENISA, ITU и EU , како на пример ISC2 CISSP, ISACA CISM, ISACA CRISC, CCSO, CIH, CES, CEH, CHFI.

## ФИНАСИСКИ ПЛАН

Планираните финансиски средства за работа на Центарот за одговор на компјутерски инциденти се утврдени во предлогот на Годишниот Финансискиот план на Агенцијата за електронски комуникации за 2017 година кој е составен дел на предлогот за Годишна програма за работа на Агенцијата за електронски комуникации.

Подолу во текстот се извадоци од предлогот за Годишен финансискиот план на Агенцијата за електронски комуникации кој се однесува за работата на Центарот за одговор на компјутерски инциденти:

Табела 3

| Конто | Опис | Износ |
|---|---|---|
| 413210/413220 | Дневници за службено патување и патни расходи – за CIRT (10% од вкупен буџет) | 844.454,00 денари |
| 416110 | Членарини во меѓународни организации организации - CIRT | 615.000,00 денари |
| 417710 | Обука и стручно усовршување - CIRT | 1.000.000,00 денари |
| 417741 | Семинари и конференции (котизација) | 350.000,00 денари |
| 417990 | Други договорни услуги – конференција и работилници во организација на АЕК/MKD-CIRT | 3.022.725,00 денари |
| 441001 | Информатичка опрема CIRT:<br>Систем за форензика<br>Систем за процена на ранливости на системи и мрежи | 5.067.730,00 денари |
| 460 | Бруто плати | 4.772.538,00 денари |

## ЗАКЛУЧОК

Во текот на 2017 година центарот за одговор на компјутерски инциденти ќе работи интензивно на исполнување на мисијата и поставените цели преку реализирање на сите предвидени акивности.

Еден од главните предизвиците во оваа година ќе биде екипирањето на тим за одговор на компјутерските инциденти и давање на подршка на сите конституенти како и нивна едукација за ефикасно извршување на задачите.

Предуслов за квалитетно и навремено пружање на услугите на MKD-CIRT за конституенитуе и граѓаните на Република Македонија е екипирање на тимот на MKD-CIRT. Нивната едукација и експертиза ќе бидат во насока на градење на доберба во квалитетот на MKD-CIRT кај конституенитите и користење на услугите.

Обезбедувањето на основните информации за подигнувањето на свеста на граѓаните за компјутерската безбедност и сајбер криминалот во овој период ќе биде основа за надградба и континуирано збогатување со нови содржини.

Во оваа година ќе биде и официјално отворена комуникацијата со останатите центри за одговор на компјутерски инциденти во регионот и пошироко.

## ВЛЕГУВАЊЕ ВО СИЛА

Годишната програма за работа на националниот центар за одговор на компјутерски инциденти, влегува во сила согласно Одлуката за нејзино усвојување од страна на Владата на Република Македонија.

Директор на
Агенција за електронски комуникации
Сашо Димитријоски

_____