Архивски број: 03-20-3791/1
Датум: 12-03-2024

Друштво за трговија и услуги
ЦПП УСЛУГИ ДОО
Бр. 0307-1771
12.03.2024 год.
СКОПЈЕ

ДОГОВОР
за јавна набавка на услуги – управувани услуги за превентивно и адаптивно одржување на сајбер безбедност

Склучен помеѓу:

1. МИНИСТЕРСТВО ЗА ФИНАНСИИ, со седиште на улица „Даме Груев“, бр.12 - Скопје, претставувано од Dr. Fatmir Besimi, министер за финансии, во натамошниот текст: договорен орган и

2. Друштво за трговија и услуги ЦПП УСЛУГИ ДОО Скопје, со седиште на ул. „ Наум Наумовски Борче“ бр.4/1, Скопје, застапувано од Филип Симеонов, управител, натамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на услуги – управувани услуги за превентивно и адаптивно одржување на сајбер безбедност, согласно со техничките спецификации (Прилог кон договорот), а по претходно спроведена поедноставена отворена постапка, по оглас број 20593/2023.

Услугата за управување со компјутерска безбедност опфаќа целокупна проценка на безбедносната зрелост на информатичката инфраструктура, проценка на сајбер отпорноста од различни софистицирани сајбер напади, следење на активностите на системите, како и креирање на препораки за подобрување на сајбер безбедноста и зголемување на нивотот на безбедност на целокупната информатичка инфраструктура на Министерството за Финансии на Република Северна Македонија.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 1.990.000,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 358.200,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 2.348.200,00 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

Цената од член 2 на овој договор е крајна, фиксна и непроменлива за цело времетраење на договорот.

IV. РОК НА ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Овој договор се склучува за период од 12 (дванаесет) месеци, а ќе започне да важи од денот на потпишувањето од двете договорни страни.

V. НАЧИН, МЕСТО И РОК НА НА ИЗВРШУВАЊЕ НА УСЛУГАТА

Член 5

Детални информации за начинот и рокот за извршување на услугата се дадени во техничките спецификации како прилог кон договорот.

Услугата ќе се извршува во Скопје.

За извршување на услугата – предмет на договорот, носителот на набавката задолжително ги вклучува лицата од стручниот кадар за извршување на услугата - предмет на договорот, согласно со прифатената понуда на носителот на набавката од страна на договорниот орган.

Во исклучителни ситуации носителот на набавката може да изврши замена на лице од техничкиот персонал кој ќе учествува во извршувањето на договорот, со доставување на детално образложение и по добивање на одобрение од договорниот орган, под услов лицето да ги исполнува условите предвидени во тендерската документација.

VI. НАЧИН И РОК НА ПЛАЌАЊЕ

Член 6

Договорниот орган плаќањето ќе го изврши во рок до 30 (триесет) дена од денот на доставувањето на фактурата со прилог извештаите предвидени во техничките спецификации прилог кон договорот.

Фактурата се доставува по пошта или лично во писарницата на Министерството за финансии, на ул.„Даме Груев" бр.12 во Скопје.

VII. ПРАВА И ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 7

Носителот на набавката е должен:

-веднаш по склучување на договорот да пристапи кон негова реализација и да ги извршува обврските стручно и квалитетно;

-да обезбеди ефикасно и навремено извршување на предметната услуга и да ги применува соодветните регулативи за конкретниот вид на услуга, придржувајќи се кон барањата на договорниот орган;

-да дава соодветни препораки за решавање на секој проблем кој би се појавил во текот на реализација на предметот на договорот;

-да му укаже на договорниот орган за било која неправилност во врска со непочитувањето на законската регулатива или било кој друг факт кој би можел негативно да влијае на исходот или очекувањата на договорниот орган и

-во рамките на извршувањето на своите обврски блиску да соработува со вработените кај договорниот орган кои ќе бидат задолжени за реализација на предметот на договорот.

Носителот на набавката се обврзува и е должен во рамките на извршувањето на своите обврски да ги смета барањата и интересите на договорниот орган кои се предмет на овој договор за приоритетни во секое време и да го информира договорниот орган, веднаш доколку се појават одредени околности кои би влијаеле на извршувањето на активностите кои се предмет на овој договор.

VIII. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 8

Договорниот орган е должен да определи лица кои ќе бидат задолжени за реализација на предметот на договорот.

Договорниот орган се обврзува дека ќе му плати на носителот на набавката за услугата, во согласност со член 6 од овој договор.

IX. ГАРАНЦИЈА ЗА КВАЛИТЕТНО И НАВРЕМЕНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 9

Носителот на набавката е должен заедно со потпишаниот договор да достави банкарска гаранција за квалитетно и навремено извршување на договорот.

Банкарската гаранција за квалитетно и навремено извршување на

договорот треба да биде во висина од 10% од вкупната вредност на договорот со пресметан данок на додадена вредност.

Гаранцијата се доставува во вид на банкарска гаранција во писмена форма или во електронска форма доколку е издадена како таква од банката во изворно оригинална форма. Гаранцијата треба да биде поднесена во оригинална форма. Копии не се прифаќаат.

Гаранцијата за квалитетно и навремено извршување на договорот треба да биде со важност до целосното реализирање на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде во валутата на која гласи договорот.

Со гаранцијата избраниот носителот на набавката гарантира дека предметот на договорот ќе го изврши на начинот и според динамиката предвидени во тендерската документација, односно техничката спецификација, доставената понуда и склучениот договор со договорниот орган.

Гаранцијата за квалитетно и навремено извршување на договорот ќе биде наплатена доколку носителот на набавката не исполни некоја од обврските од договорот за јавна набавка во рокот на стасаноста, за што писмено ќе го извести носителот на набавката.

Доколку договорот за јавна набавка е целосно реализиран согласно договореното, банкарската гаранција за квалитетно извршување на договорот договорниот орган му ја враќа на носителот на набавката во рок од 14 дена од целосното реализирање на договорот.

Гаранцијата за квалитетно и навремено извршување на договорот договорниот орган му ја враќа на носителот на набавката по пошта, лично во седиштето на носителот на набавката или лично во седиштето на договорниот орган.

Договорниот орган ќе ја наплати гаранцијата за квалитетно и навремено извршување на договорот и доколку дојде до негово едностране раскинување поради неизвршување на обврските од договорот од страна на носителот на набавката.

Договорниот орган нема да бара активирање на банкарската гаранција за квалитетно извршување на договорот од банката која ја има издадено доколку носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) не можел да ја изврши набавката што е предмет на овој договор, во кој случај носителот на набавката треба да достави писмено образложение до договорниот орган во кое ќе ги наведе причините за неизвршување или ненавремено извршување на набавката, а кое треба да биде писмено прифатено од договорниот орган.

X. ДОВЕРЛИВОСТ НА ПОДАТОЦИ И ИНФОРМАЦИИ

Член 10

Определените лица од носителот на набавката наведени во понудата за реализација на договорот, задолжително потпишуваат изјава за доверливост на информации и податоци непосредно пред извршувањето на услугата - предмет на договорот.

Под поимот информации и податоци се подразбираат сите внатрешни и надворешни документи, спецификации, лични податоци, истражувања на пазарот или податоци за него, финансиски или маркетиншки информации, други податоци или бизнис, оперативни или технички информации, како и сите останати податоци и информации и независно дали се дадени во писмена, вербална или електронска форма и се во сопственост на договорниот орган.

Исто така, поимот информации и податоци, ги опфаќа и сите други податоци кои не се сопственост на договорниот орган, а се користат за одредени цели во работните задачи и обврски. Тука спаѓаат податоци на сите партнери, клиенти, добавувачи или било кое правно или физичко лице кое со Договорниот орган има засновано деловен или било каков друг однос. Договорниот орган ги става податоците на располагање на носителот на набавката во врска со погоре наведената цел, а за непречено одвивање на работните задачи и обврски.

Член 11

Не се предмет на овој договор информации кои биле или станале јавно достапни, но не како резултат на откривање од страна на носителот на набавката и на договорниот орган и без да бидат прекршени одредбите на овој договор од страна на носителот на набавката што може да се докаже со писмена документација или за кои договорниот орган писмено потврдил дека се ослободени од обврска за неоткривање.

Член 12

Носителот на набавката под целосна морална, материјална и кривична одговорност, се обврзува за време на важноста на договорот и во период од (5) пет години од датумот на неговото истекување или раскинување да ги чува во тајност сите информации и податоци од било која област на договорниот орган, кои ќе му бидат дадени во процесот на соработката и притоа нема да ги искористи истите за лични цели, во име на друго лице, ниту ќе ги даде на увид на трета страна.

Носителот на набавката се обврзува да ги чува во тајност сите документи и податоци кои содржат информации за договорниот орган или неговите активности, како и неговите односи со клиенти или трети лица, а кои биле

подготвени или изнесени во врска со работата за која Носителот на набавката е ангажиран од страна на договорниот орган.

Член 13

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 10 став 2 и 3 заради постапување по писмено барање од страна на надлежен орган, со легитимна наредба врз основа на закон.

Носителот на набавката, пред да ги даде бараните податоци ќе се увери дека барањето е валидно и е во согласност со важечки закон и ќе ги открие ваквите податоци само до степен до кој тоа е барано од надлежниот орган кој има овластување да бара такво соопштување.

Член 14

За секој настан или сомневање во однос на закана за нарушување на доверливоста, интегритетот и расположливоста на податоците и информациите, носителот на набавката се обврзува веднаш писмено да го извести определеното лице кај договорниот органот.

Член 15

Носителот на набавката по писмено барање на договорниот орган веднаш ќе ги врати или уништи сите документи кои содржат податоци и информации за договорниот орган, а кои се добиени во врска со работата за која носителот на набавката е ангажиран од страна на договорниот орган, без задржување на било какви фотокопии, изводи или друг вид на копии од нив или дел од нив. И покрај уништувањето на било кој податок и материјали носителот на набавката ќе продолжи да се придржува кон неговата обврска од овој договор и други обврски кои произлегуваат од него, за чување во тајност на сите податоци и информации кои ги сознал на било кој начин, при исполнување на неговите обврски кои произлегуваат од овој договор.

Член 16

Објавувањето податоци, рекламирањето или публицитетот, како и прес конференциите направени од страна на Носителот на набавката во однос на овој договор или вршење на заеднички деловни активности на договорните страни треба да бидат претходно одобрени од договорниот орган пред нивното спроведување.

Член 17

Одредбите од глава X од овој договор се правно валидни и обврзувачки и кај сите вработени кај носителот на набавката кои имаат добиено овластување за користење на информациите и податоците кои се уредени со овој договор.

XI. УСЛОВИ ЗА ПРЕКИНУВАЊЕ ИЛИ РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 18

Овој договор може да се раскине спогодбено во согласност на двете договорни страни.

Член 19

Овој договор може да се раскине и едностранo поради непридржување или неисполнување на договорните обврски утврдени со овој договор.

Договорната страна која поради непридржување или неисполнување на договорните обврски го раскинува договорот, должна е тоа да и го соопшти на другата договорна страна без одлагање во писмена форма.

Договорот се смета за раскинат со денот на приемот на известувањето за раскинување на договорот.

Доколку дојде до раскинување на договорот поради неисполнување или ненавремено исполнување на обврските на договорот од страна на носителот на набавката, покрај наплата на банкарската гаранција за квалитетно и навремено извршување на договорот, носителот на набавката ќе биде одговорен и за евентуалната штета што би ја предизвикал на договорниот орган како директна или индиректна последица на неговото работење.

Член 20

Кога една од договорните страни нема да ја исполни својата обврска, договорната страна може да бара исполнување на обврската од другата договорна страна или да го раскине договорот, и да ја активира банкарската гаранција за квалитетно и навремено извршување на договорот, а во секој случај има право на надомест на штетата.

Член 21

Кога договорната страна нема да ја исполни својата обврска во определениот рок, другата договорна страна може да и остави примерен дополнителен рок за исполнување на обврската.

Рокот од став 1 на овој член може да биде продолжен само по писмено барање на носителот на набавката и писмена согласност од договорниот орган.

Ако договорната страна која не ја исполнила својата обврска во определениот рок, не ја исполни обврската ни во дополнителниот рок, другата договорна страна може да го раскине договорот.

XII. ВИША СИЛА

Член 22

Ниту една од договорните страни нема да биде одговорна за неисполнување на обврските од овој договор до кое би дошло заради виша сила.

Под виша сила се подразбираат настани или околности на кои договорните страни не можат да влијаат и се надвор од нивната контрола, а го попречуваат нормалното извршување на договорот (елементарни непогоди, воени дејства, граѓански немири, штрајкови и сл.).

Вишата сила не вклучува настан што е предизвикан од небрежност или намерна активност што би предизвикала застој во извршувањето на обврските од договорот.

Ако една од договорните страни е спречена да ги исполнува своите обврски заради виша сила, должна е веднаш писмено да ја извести другата страна, со наведување на причините за вишата сила и по можност обезбедување на соодветен доказ.

За времетраењето на вишата сила сите права и обврски од овој договор мируваат.

Договорните страни се обврзуваат на ист начин да ја известат договорната страна за повторното воспоставување на нормални услови за извршување на договорот, односно за престанокот на дејството на вишата сила.

По отстранувањето на вишата сила договорот продолжува да се реализира.

XIII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 23

Изменувања и дополнувања на договорот можат да се вршат со заедничка согласност на договорните страни по писмен пат.

Договорната страна која бара измена и/или дополнување на договорот е должна своето барање до другата страна да го достави во писмена форма.

Договорот може да се изменува и дополнува со анекс на договорот потпишан од двете договорените страни во согласност со Законот за јавните набавки.

Член 24

За сé што не е предвидено со овој договор, се применуваат одредбите од Законот за облигационите односи, Законот за јавните набавки и од другите позитивни прописи во Република Северна Македонија.

Член 25

Во случај на спор, договорните страни се согласни спорот да го решат спогодбено, а доколку во тоа не успеат, согласни се спорот да го решава предметно надлежниот суд во Скопје.

Член 26

Обработката на личните податоци при реализацијата на овој договор ќе биде во согласност со Законот за заштита на личните податоци.

Член 27

Овој договор е составен во 4 (четири) еднообразни примероци од кои 2 (два) примероци за договорниот орган и 2 (два) за носителот на набавката.

ДОГОВОРЕН ОРГАН:
РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

МИНИСТЕРСТВО ЗА ФИНАНСИИ
СКОПЈЕ

МИНИСТЕР ЗА ФИНАНСИИ
Dr. Fatmir Besimi

НОСИТЕЛ НА НАБАВКАТА:
Друштво за трговија и услуги

ЦПП УСЛУГИ ДОО Скопје

УПРАВИТЕЛ
Филип Симеонов

Друштво за трговија и услуги ЦПП УСЛУГИ ДОО СКОПЈЕ

Изработил: Панче Чоневски
Контролирал: Даниела Јанкова
Елизабета Калачоска
Одобрил: Татјана Васева
Проверил: Daut Hajrullahi
м-р Маја Стаменковска Угриновска
Љубомир Јорданов
Согласен: д-р Јелена Таст

ТЕХНИЧКИ СПЕЦИФИКАЦИИ ПРИЛОГ КОН ДОГОВОР

Услугата за управување со Компјутерска безбедност потребно е да опфати целокупна проценка на безбедносната зрелост на информатичката инфраструктура, проценка на сајбер отпорноста од различни софистицирани сајбер напади, следење на активностите на системите, како и креирање на препораки за подобрување на сајбер безбедноста и зголемување на нивотот на безбедност на целокупната информатичка инфраструктура на Министерството за Финансии на Република Северна Македонија.

Во рамки на оваа услуга економскиот оператор потребно е да ги покрие следните активности со цел да се покрие целокупната сајбер безбедност на министерството, а тоа се:

-Надворешно и Внатрешно Пенетрациско тестирање
-Ре-тест на најдени ранливости по ремедијација во рамки на 1 година
-Интеграција на нови и унапредување на постојните извори на настани во систем за централно логирање на безбедносни настани
-Мониторинг на настани и аларми од системот за централно логирање на безбедносни настани до 2 часа/дневно
-Дедицирано лице за сајбер безбедност на далечина/на лице место до 20 часа/месечно
-Дефинирање и креирање на предупредувања и правила за корелација според најдобрите безбедносни практики и деловни процеси
-Следење на Здравјето на системот за централно логирање на безбедносни настани(4 пати месечно)
-Квартална проценка на безбедноста на внатрешната инфраструктура и проценка на ранливости
-Месечно скенирање за ранливост на сите надворешно изложени системи
-Следење на настани и закани преку threat intelligence за институцијата и надворешно изложените системи и сервиси
-Препораки за митигација и ремедијација на одредени пропусти и слабости во системите
-Напредна анализа на постоечки и нови ранливости
-Тим за одговор по инциденти 24/7 до 2 инциденти месечно
-Консултантски услуги за сајбер безбедност до 10 часа месечно
-Обука за безбедност на свеста за вработените (дигитализирана)

Опис на активностите:

- **Надворешно и Внатрешно Пенетрациско тестирање**

Проверката на сигурноста од пробивање (penetration testing) на Надворешната и Интерната ИТ инфраструктура вклучувајќи го и трезорот и неколку критични веб апликации сопственост на Министерство за Финансии треба да опфати фокусирана проверка на безбедноста на надворешната и интерната компјутерска мрежа, проверка на надворешните и внатрешните заштити и критичните системи и веб апликации преку кое ќе се добие објективна слика за нивото на безбедност одделно на секој од сегментите во инфраструктурата, односно ќе се направат реални проверки на сигурносните

контроли од интернет и од внатрешна мрежа симулирајќи реални хакерски напади од надворешни лица или интрудери.
Проверката треба да биде извршена целосно длабински, имајќи ги во предвид сите компоненти кои се дел од надворешната и внатрешната ИТ инфраструктура.

Начин на работа

Двата типа на тестирање треба да бидат поделени во две фази на проверката на сигурноста од пробивање и тоа:

- Прва фаза (Надворешно Пенетрациско Тестирање) - Пристап од интернет без познавање на информации за ИТ инфраструктурата. (симулација на хакер од интернет кој употребува реални хакерски напади). Првата фаза ќе ги опфати сите надворешни сервиси и системи со кои располага организацијата и истите ќе бидат предмет на проверка и тестирање согласно однапред дефинирана методологија. Тестирањето ќе биде по принцип на црна кутија односно без овозможување на пристап преку моменталните заштитни контролни механизми на организацијата. Во првата фаза потребно е да се опфатат и тестирање на неколку критични веб апликации кои ќе бидат откриени на економскиот оператор што ќе ја добие набавката заради доверливост.

- Втора фаза (Внатрешно Пенетрациско Тестирање) - Пристап од интранет мрежата со ограничени информации (Симулација на напад од регуларен корисник, односно вработен во институцијата или интрудер во рамките на интерната мрежа). Втората фаза ќе ги опфати сите интерни критични системи и мрежни уреди, внатрешната мрежна инфраструктура и апликации кои имаат пристап само до интерна мрежа и вработени во институцијата. Тестирањето ќе биде по принцип на Сива кутија согласно однапред дефинирана методологија.

Проверката на системот не смее да ја наруши функционалноста на целиот систем (неинтрузивен метод). Доколку се откриени слабости кои можат да се искористат за нарушување на сигурноста на информацискиот систем (exploits), потребно е да се достави детален план за искористувањето на овие слабости, кој треба да биде одобрен од Министерство за Финансии, пред истите да се употребат. При тоа слабостите треба да се рангираат согласно методологијата дефинирана во техничката документација. Правото да се прифати откриената слабост без употреба на искористувач (exploit) го задржува Министерството за Финансии доколку постои голем ризик за нарушување на оперативноста на информатичкиот систем.

Доколку економскиот оператор има функционално имплентирано решение (софтвер или хардвер) кое е во продукциска околина кај договорниот орган или има активен договор на одржување на некој дел од компјутерскиот систем како изведувач или подизведувач, не може да учествува во предметната набавка.

Производ од проверката

Како резултат на проверката на сигурноста од пробивање на надворешните и внатрешните системи, како и на интерната мрежа на Министерство за Финансии, понудувачот треба да достави:

- Извештај на крај на изведба на сите фази од пенетрациското тестирање во кој најмалку ќе се содржи опис на начинот на работа, извршените тестирања, наоди за откриените слабости, нивен детален опис и рангирање, доказ за откриените слабости, како и детален начин за отстранување на истите.
- Сеопфатен краен извештај за проверката, изготвен по завршување на последната фаза, во кој ќе е опфатена целата проверка (сите фази), во кој најмалку ќе се содржи опис на начинот на работа, извршените тестирања и користени алатки, наоди за откриените слабости, нивен детален опис и рангирање, доказ за откриените слабости, како и детален начин за отстранување на истите. Крајниот извештај треба да е поделен на две независни целини од кои првата е наменета за раководството на Министерство на Финансии со сумарни информации а втората е наменета за оперативниот кадар на Министерство за Финансии и содржи технички детали.
- Препораки и консултации за имплементација на безбедносни решенија за зголемување на нивото на безбедност на системите, услугите и вработените за поголема контрола врз целокупното работење на организацијата.

Членовите од тимот наведени во техничка и професионална способност треба да бидат вклучени во дневните активности додека други членови од тимот кои се дополнително наведени може да бидат вклучени во дневните активности само како дополнителни консултанти придружувани од главните членови на тимот.

Рангирањето на наодите треба да се изврши врз основа на OWASP RISK RATING METHODOLOGY **(*https://owasp.org/www-community/OWASP_Risk_Rating_Methodology)**

*Извештаите генерирани како резултат од тестирањето потребно е да бидат на македонски јазик.

-Ре-тест на најдени ранливости по ремедијација во рамки на 1 година

Проверка на исполнување на препораките за сите пронајдени ранливости и слабости на информатичкиот систем по нивно затворање односно по нивна ремедијација од страна на тимот одговорен за одржување на компјутерска и мрежна инфраструктура, вклучувајќи го и апликативното одржување.

-Интеграција на нови и подобрување на постојните извори на настани во систем за централно логирање на безбедносни настани

Креирање и подобрување на конектори за собирање на безбедносни настани од нови и постојни системи, мрежни уреди и апликации кои се дел од информатичката инфраструктура на Министерството за Финансии, согласно можностите за интеграција на достапни безбедносни настани (логови) кои постојат во самите апликации.

-Мониторинг на настани и аларми од системот за централно логирање на безбедносни настани до 2 часа/дневно

Економскиот оператор ќе прави редовен мониторинг на системот за централно собирање на настани и на системот за крајна заштита (end-point) од појава на потенцијални напади и злонамерни активности на системско, мрежни и апликативно ниво и истиот ќе функционира подреден на 3 улоги поделени по нивоа и тоа,
Ниво 1 - задолжен за детектирање, тријажа и решавање на инцидент во информациониот систем,
Ниво 2 - задолжен за решавање на напредни инциденти, одговор по инциденти и дигитална форензика
Ниво 3 – задолжен за ловење на закани, креирање на напредни и корелации на правила за познати и непознати закани.

Сите улоги потребно е да работат заеднички и како тим да ги решаваат сите потенцијални инциденти и навремено ги информираат одговорните лица од институцијата преку одреден систем за пријава на компјутерски инцидент.

-Дедицирано лице за сајбер безбедност на далечина/на лице место до 20 часа/месечно

Економскиот оператор ќе обезбеди и дедицира лица за сајбер безбедност кои ќе биде на располагање за било какви прашања, конфигурации или препораки од областа на сајбер безбедноста. Надворешното лице исто така може да биде вклучено и во евалуација и креирање на архитектури за набавки на продукти за сајбер безбедност во рамки на институцијата.

-Дефинирање и креирање на предупредувања и правила за корелација според најдобрите безбедносни практики и деловни процеси

Економскиот оператор потребно е да крерира листа на правила, аларми и активности кои ќе бидат поставени во рамки на информациониот систем и системот за следење на активности преку креирање на playbooks за полесно и навремено откривање на

потенцијални напади и злонамерни активности во интерниот и надворешниот информационен систем на институцијата.

-Следење на Здравјето на системот за централно логирање на безбедносни настани(4 пати месечно)

Економскиот оператор потребно е да го следи здравјето на системот за централно логирање на безбедносни настани од аспект на број на настани по секунда, слободна меморија, функционални конектори, CPU, архивирање.

-Квартална проценка на безбедноста на внатрешната инфраструктура и проценка на ранливости

Економскиот оператор е должен секој квартал во рамки на 1 година да врши скенирање за ранливости на сите критични системи во информатичката инфраструктура со комерцијален скенер за откривање на ранливости и како резултат да креира акциски план за решение на пронајдените ранливости.

-Месечно скенирање за ранливост на сите надворешно изложени системи

Економскиот оператор е должен еднаш месечно да изврши скенирање за ранливости на сите надворешно изложени системи и да креира извештај за пронајдените ранливости заедно со препораки за нивно решавање.

-Следење на настани и закани преку threat intelligence за институцијата и надворешно изложените системи и сервиси

Постојано следење и детектирање на потенцијални закани и настани од јавно публикувани извори, социјални медиуми, детектирање на фишинг напади, dark web истражувања кои се поврзани со домеини и сретства на институцијата. Активноста исто така треба да покрива и откривање на 0-day ранливости и закани од кои можат да бидат афектирани системите и заштитните уреди на институцијата.

-Препораки за митигација и ремедијација на одредени пропусти и слабости во системите

Економскиот оператор задолжен за сајбер безбедноста на информатичката инфраструктура потребно е за секоја закана, пропуст, слабост или пронајдена ранливост да креира мерки и препораки за истата да биде затворена односно да предложи решение за одбрана од потенцијалната закана, пропуст, слабост или ранливост.

-Напредна анализа на постоечки и нови ранливости

Економскиот оператор потребно е секоја нова или постоечка ранливост детално да ја анализира и да провери дали е апликабилна на некој од системите од институцијата, односно дали провери дали ранливоста може да биде искористена од страна на трети лица со цел компромитација на системот и нарушување на неговата редовна работа.

-Тим за одговор по инциденти 24/7

Економскиот оператор е потребно да обезбеди тим за одговор по инцидент 24/7 односно достапни ресурси во случај на настанат компјутерски инцидент од далечна локација и на лице место и ќе биде задолжен да го исполни следниот договор на ниво на активност за одговор по инцидент.

1. Првичниот одговор на инцидент со висок приоритет во рок од 30 минути доколку може да се одговори од далечинска локација;
2. Првичниот одговор на инцидент со висок приоритет во рок од 90 минути доколку е потребно да се одговори на сама локација; Доколку е потребно да се одговори на локација оддалечена повеќе од 50км, времето на одзив ќе биде 4 часа.
3. Првичната проценка на инцидентот во рок од 2 часа.
4. Потполно отстранување на инцидентот во рок од 4 часа.
5. Разрешување на инцидентот во зависност од големината и тежината на инцидентот
6. Преглед и известување по инцидентот во рок од 72 часа доставено до министерството за образование и наука;
7. Првичен извештај за настанат инцидент во рок од 3 дена по решавањето на инцидентот.

-Консултантски услуги за сајбер безбедност до 10 часа месечно

Економскиот оператор потребно е да има советодавна улога од типот на воспоставување на безбедносна архитектура на системи, мрежи и апликации, воспоставување на безбедносни стандарди и политики, креирање на безбедносни политики и процедури, избор на безбедносни решенија.

Обука за безбедност на свеста за вработените (дигитализирана)

Економскиот оператор потребно е да поседува или воспостави платформа за online обуки за зголемување на свеста за сајбер безбедност и истата да биде 24/7 достапна за сите вработени во институцијата. Платформата потребно е да има можност за видео обука, полагање на испит и издавање на сертификат за успешно завршена обука за зголемување на свеста на сајбер безбедност. Пристап до обуката треба да имаат сите вработени 24/7/365 со времетраење од минимум 45 минути и истата да има можност за генерирање на извештај за сите завршени обуки и посети за вработените во министерството, со време на присуство, датум, положен или не, издаден сертификат.