РЕПУБЛИКА МАКЕДОНИЈА
ДИРЕКЦИЈА ЗА БЕЗБЕДНОСТ
НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

МЕТОДОЛОГИЈА

за изработка на процена на ризик за информатичка безбедност[1]

ОДОБРУВА
Директор
д-р Александар Нацев

Digitally signed by Aleksandar Nacev
Date: 2017.02.21 09:59:59 CET

Скопје
февруари, 2017 година

[1] Проект финансиран од Мисијата на ОБСЕ во Скопје, Република Македонија

СОДРЖИНА

1. ВОВЕД

Еден од клучните елементи на одржлива безбедност на комуникациско-информатичките системи во кои се процесираат класифицирани информации е проценатa на ризикот. Целта на проценатa е да го координира и да го оптимизира користењето ресурси и да ги мониторира, да ги контролира и да ги минимизира заканите што може да ја нарушат безбедноста. Преку спроведување процена на ризик најпрво на институционално, а потоа и на национално ниво и преку синхронизирање со националните безбедносни потреби, се идентификуваат најважните закани во поглед на информатичката безбедност.

Дизајнирањето на методологија на процена на ризик за информатичка безбедност не е воопшто лесна активност, особено ако се земе предвид дека таа треба да биде функционална и применлива во дивергентни институционални и национални рамки. т.е во широка лепеза на институции што се разликуваат: според вид на сектор (државен, приватен, непрофитен), според број на кадар (големи, средни, мали), според вид на дејност (безбедност, економија, наука, култура). Со оглед на тоа дека информатичката безбедност во поново време е од исклучителна важност особено за институциите што ѝ припаѓаат на националната критична инфраструктура, а најмногу за институциите/организациите што процесираат класифицирани информации низ комуникациско-информатички системи, оваа методологија за изработка на процена на ризик за информатичка безбедност ќе најде примена кај безбедносните институции – чинители на безбедносниот систем на Република Македонија, кај државните органи што придонесуваат во целост или во некој домен во безбедноста, кај банкарско-финансиските институции и компании што поседуваат комуникациско – информатички системи за пренос на информации, кај компаниите од електроенергетскиот, хидроенергетскиот, телекомуникацискиот, воено-индустрискиот, транспортниот, информациско-технолошкиот сектор и други. Исто така, оваа методологија може да се користи и од страна на сите лица што се активно вклучени и/или одговорни за подготвување безбедносно-одбранбени стратегии, планови, програми, извештаи, процени за ризик, како и за лицата-безбедносни офицери задолжени за безбедност на вработените, на опремата, на имотот и на целокупната инфраструктура во своите матични организации од државниот и од приватниот сектор. Притоа не треба да се заборави дека секоја организација или институција поседува различни финансиски, технички, материјални, организациски и човечки капацитети, па оттука и

потребата на адаптирање на методологијата во согласност со своите ресурси и потреби.

Фокусот на овој документ за процена на ризик е ставен на ризикот што се разгледува низ призмата на неговите главни конституенти: *идентификација на ризик, анализа на ризик и евалуација на ризик.* Покрај општите појаснувања за овие три елементи што всушност ја сочинуваат проценатa на ризик, оваа методолошки средена алатка со помош на дијаграми, табели и матрици едноставно и практично го прикажува текот на проценатa на ризик во една институција. Исто така, овој документ го третира управувањето со ризикот и претставува своевидна безбедносна анализа којашто пропишува мерки и процедури за информатичка безбедност. Со користење на повеќеслоен аналитички пристап ризикот се разгледува не само од гледна точка на информатичката безбедност, туку и од гледна точка на физичката, па дури и на персоналната безбедност.

2. Процена на ризик за информатичка безбедност

Проценатa на безбедносниот ризик е процес на идентификација на безбедносен ризик, односно идентификација на ранливостите и заканите, како и одредување контрамерки за тие закани. Проценатa на безбедносниот ризик придонесува за донесување прецизна одлука за избор на вистинската мерка за заштита на сопствените ресурси.

2.1. Генерален (општ) опис на проценатa на ризик за информатичка безбедност

Ризикот е комбинација од последиците што ќе следат по случувањето на несакан настан и веројатноста од случувањето на настан. Проценатa на ризикот квантитативно или квалитативно го објаснува ризикот и им овозможува на раководните лица да им дадат приоритет на ризиците врз основа на нивното согледување на сериозноста или други воспоставени критериуми. Проценатa на ризикот се состои од следните активности: **идентификација на ризикот, анализа на ризикот и евалуација на ризикот.** Проценатa на ризикот ја одредува вредноста на информатичките ресурси (средства), ги идентификува променливите закани и ранливости што постојат (или може да постојат), ги идентификува постојните контроли и нивниот ефект врз идентификуваниот ризик, ги одредува потенцијалните последици и на крај ги приоритизира добиените ризици и ги рангира во однос на критериумите за евалуација на ризикот утврдени во контекст на воспоставување.

2.2. Идентификација на ризикот

2.2.1. Вовед во идентификацијата на ризикот

Целта на идентификацијата на ризикот е да одреди што може да се случи за да се предизвика потенцијална загуба и да се добие увид во тоа како, каде и зошто загубата може да се случи. Идентификацијата на ризикот треба да вклучува ризици на кои изворот им е или не им е под контрола на организацијата, дури и ако изворот или причината за ризикот не се очигледни.

2.2.2. Идентификација на критичните ресурси

Опис на активноста: ресурс (средство) е сè што има вредност за институцијата и поради тоа има потреба од заштита. За идентификација на

ресурсите треба да се има предвид дека информатичкиот систем се состои од многу повеќе елементи, а не само од хардвер и софтвер. Идентификацијата на ресурсите треба да се спроведе на соодветно ниво на детаљност што овозможува доволно информации за проценатa на ризикот. Нивото на детаљност што ќе се користи за идентификација на ресурсот ќе влијае на целокупната количина на информации собрани за време на проценатa на ризикот. Корисникот на ресурсот треба да биде идентификуван со цел да се обезбеди одговорност и отчетност за ресурсот. Многу често корисникот на ресурсот е најсоодветната личност за да ја одреди вредноста на ресурсот за институцијата.

Очекуван резултат: Листа на ресурси што треба да бидат земени предвид во однос на ризиците и Листа од работни процеси поврзани со ресурсите и нивната релевантност (Види: Додаток 1 - Идентификација и вреднување на критичните ресурси и процена на влијанието).

2.2.3. Идентификација на заканите

Опис на активноста: идентификацијата на заканата треба да потекне од вработените во организацијата и од безбедносните органи. За секоја закана треба да се идентификува: изворот, целта, намерата, мотивот, капацитетот на заканата и последиците што би ги предизвикала.

Заканата има потенцијал да им наштети на ресурсите, како што се: информациите, процесите и системите, и следствено на тоа на организациите. Заканите може да бидат од природно или од човечко потекло и може да бидат случајни или намерни. И случајните и намерните извори на закани треба да бидат идентификувани. Заканата може да произлезе и од внатре и од надвор на организацијата. Заканите треба да бидат идентификувани генерички и според типот како индивидуални закани во рамките на идентификуваната генеричка класа.

Некои закани може да влијаат на повеќе од еден ресурс. Во таков случај тие може да предизвикаат различни влијанија во зависност од тоа кој ресурс е засегнат. Информации за идентификацијата на заканата и проценатa за веројатноста за случување можат да се добијат од корисниците на ресурсите, од персоналот за човечки ресурси, од експертите за информатичка безбедност како и од експертите за физичка безбедност.

Исто така, кога се зборува за заканите, треба да се земат предвид и аспекти од околината (животната средина) и културата. Треба да се земат предвид и закани специфични за институцијата, за да се комплетира листата

со генерички закани. Внатрешни искуства од инциденти и претходни процени на закани треба да се земат предвид во тековната процена. Кога се користат листи на закани или резултати од претходни процени на ризик, треба да се има предвид дека постои континуирана промена на релевантните закани, особено ако безбедносната околина или информатичките системи се менуваат. За илустрација на разните видови закани, во следната табела се дадени пример на листа на закани и пример на нивно градирање на ниско, на средно и на високо ниво.

Очекуван резултат: Листа на закани со идентификација на типот на изворот на закана (Види: Додаток 2 - Примери на типични закани).

2.2.4. Евалуација на постојни безбедносни контроли

Опис на активноста: Треба да се спроведе евалуација на постојните безбедносни контроли на КИС за да се избегне непотребна работа или трошоци, на пример, при дуплирање на контролите. Дополнително, додека се идентификуваат постојните контроли, треба да се направи проверка за да се осигура дека контролите даваат резултат. Ако контролата не функционира како што е очекувано, таквата ситуација може да предизвика ранливости.

Треба да се земе предвид ситуација во која одредена контрола нема да функционира и поради тоа се потребни дополнителни контроли за ефективно справување со идентификуваниот ризик. Начин да се процени ефектот од контролата е да се види како таа ја намалува веројатноста на ризикот и леснотијата за искористување на ранливоста или влијанието на инцидентот.

Постојната или планирана контрола може да се идентификува како неефективна или неоправдана. Во тој случај, контролата треба да се провери за да се утврди дали треба да се отстрани или да се замени со друга посоодветна контрола.

Очекуван резултат: Листа на постојни и планирани контроли, нивна имплементација и статусот на употреба.

2.2.5. Идентификација на ранливости

Опис на активноста: Треба да се идентификуваат ранливостите што може да бидат искористени од заканите за да предизвикаат штета на ресурсите или на институцијата. Ранливостите може да бидат идентификувани во следните области:

- институционална оперативност;

- процеси и процедури;
- управувачки рутини;
- персонал;
- физичко окружување;
- конфигурација на информатичкиот систем;
- хардвер, софтвер или комуникациска опрема и
- зависност од надворешни страни (субјекти, фактори).

Присуството на ранливост не предизвикува штета само по себе, бидејќи треба да постои закана што би ја искористила таа ранливост. И обратно, закана што нема соодветна ранливост што би можела да ја искористи може да не резултира во ризик. Ранливостите може да се поврзат со својствата на ресурсот што може да се користат на начин или за намена различна од таа која била предвидена кога ресурсот е ставен во употреба.

Очекуван резултат: Листа на ранливости поврзани со средствата, заканите и контролите (Види: Додаток 3 – Преглед на ранливости).

2.2.6. Идентификација на последиците

Опис на активноста: Треба да се идентификуваат последиците по губењето на доверливоста, интегритетот и достапноста на ресурсите. Последица може да биде губење на ефективноста, неповолни услови за работа, загуба на работа, репутација, штета итн.

Оваа активност ја идентификува штетата или последиците врз институцијата што може да бидат предизвикани од безбедносно нарушување. Безбедносно нарушување е закана што искористува одредена ранливост или група ранливости во нарушување на информатичката безбедност. Безбедносното нарушување може да има ефект врз еден или врз повеќе ресурси или на дел од тој ресурс. Последиците можат да бидат од временска природа или трајни (како, на пример, во случај на уништување на ресурсот).

Институциите треба да ги идентификуваат оперативните последици од безбедносните нарушувања во однос на:

- истрага и време на поправка;
- загуба на (работно) време;
- загуба на можност;

- здравје и безбедност;
- финансиски трошоци за специфични вештини за поправка на штетата и
- приказ на репутацијата и добрата волја.

Очекуван резултат: Листа на очекувани последици од настанато безбедносно нарушување.

2.3. Анализа на ризикот

Анализата на ризикот, како составен дел од проценатa на ризик, може да се изврши во различни степени во зависност од критичноста на ресурсот, степенот на ранливост, пред инцидентите да се случат во институцијата.

2.3.1. Методологии за анализа на ризик

Методологијата за анализа на ризик може да биде квалитативна или квантитативна, или комбинација од двете, во зависност од околностите. Во пракса, квалитативната анализа често се користи прва за да се добие општ показател за нивото на ризик и да се откријат главните ризици. Подоцна може да биде неопходно да се преземат поспецифични или квантитативни анализи на главните ризици, бидејќи квалитативната анализа обично е помалку сложена и помалку скапа да се спроведе отколку квантитативна анализа. Формата на анализа треба да биде во согласност со критериумите за процена на ризикот развиени како дел од воспоставувањето на контекст.

(а) Квалитативна анализа на ризик

Квалитативната анализа на ризикот користи скала од квалификациски атрибути за да се опише големината на потенцијалните последици (на пример, ниска, средна и висока) и веројатноста дека ќе се случат тие последици. Предноста на квалитативната анализа е нејзината леснотија во разбирање од страна на сиот релевантен персонал, додека недостатокот е во зависноста од субјективниот избор на скалата.

Овие скали може да се приспособат да одговараат на околностите и за различни ризици може да се користат различни објаснувања. Квалитативна анализа на ризикот може да се користи:

- како почетен преглед на активности за да се идентификуваат ризиците што бараат подетаљна анализа;
- како анализа соодветна за одлуки и

- кога нумеричките податоци или ресурси се несоодветни за анализа на квантитативни ризици.

Квалитативната анализа треба да користи фактички информации и податоци секаде каде што е возможно.

(б) Квантитативна анализа на ризик

Квантитативната анализа на ризик користи скала со нумерички вредности (за разлика од квалитативна анализа на ризик каде се користат описни скали) за последиците и веројатноста, со користење податоци од различни извори. На квалитетот на анализата влијае точноста и комплетноста на нумеричките вредности и валидноста на користените модели. Квантитативна анализа на ризикот во повеќето случаи користи историски податоци за нарушувањето, обезбедувајќи предност што може да се поврзе директно со целите на безбедноста на информациите и интересите на институцијата. Недостатокот на овој вид анализа е немањето податоци за нови ризици или нови слабости што влијаат врз безбедноста на информациите. Недостаток на квантитативниот пристап може да биде кога фактички (суштински, битни), проверливи податоци не се достапни, а со тоа се создава илузија за вредноста и точноста на изработената процена на ризикот. Начинот на кој последиците и веројатноста се изразени и комбинирани за добивање соодветно ниво на ризик, ќе се разликуваат во зависност од видот на ризикот и целта за која резултатот од проценатa на ризикот ќе се користи. Несигурноста и променливоста на последиците и веројатноста треба да се разгледуваат ефективно во самата анализа.

2.3.2. Процена на последиците

Опис на активноста: По идентификација на сите ресурси што се под изложеност на ризиците, треба да бидат земени предвид вредностите на овие ресурси при проценување на последиците. Вреднувањето на ресурсите започнува со класификацијата според нивната критичност, во смисла на тоа колку се значајни тие за исполнување на целите на работењето на организацијата. Вреднувањето потоа се определува со помош на две мерки:

- вредност за замена на ресурсот: цената за обновување и замена на информациите (ако воопшто е можно) и
- последиците од губење или компромитирање на ресурсот, како што се потенцијални негативни влијанија врз работата и/или правни или регулаторни последици од откривање,

модифицирање, недостапност и/или уништување на информации, како и други информатички средства.

Вреднување на средствата е клучен фактор на влијанието на безбедносното нарушувањето во проценатa, бидејќи нарушувањето може да влијае на повеќе од еден ресурс. Различни закани и слабости ќе имаат различни ефекти врз ресурсите, како што се губење доверливост, интегритет и достапност.

Последиците може да бидат изразени во однос на финансиските, техничките или човечките критериуми или пак други критериуми релевантни за институцијата. Во некои случаи повеќе од една нумеричка вредност е потребна за да се одредат последиците за различни времиња, локации, групи или ситуации.

Очекуван резултат: Листа на оценетите последици од безбедносното нарушување изразени во однос на ресурсите и на критериумите за влијание.

2.3.3. Процена на веројатноста на безбедносното нарушување

Опис на активноста: По идентификација на безбедносните нарушувања, потребно е да се процени веројатноста да се случи некое нарушување, преку користење на техниките на квалитативна или на квантитативна анализа. Овде треба да се земе предвид колку чести се заканите и колку лесно може да се искористат слабостите, со оглед на:

- искуства и статистички веројатности за заканите;
- намерни извори на закани: мотивација и способности, што се променливи со текот на времето, ресурсите достапни за можните напаѓачи, како и перцепцијата на атрактивноста и ранливоста на средства за тие напаѓачи кон системите;
- за случајни извори на закана: географски фактори, на пример, близина на хемиската или нафтената индустрија, екстремни временски услови и фактори што може да влијаат врз појава на човечки грешки и дефекти на опремата;
- ранливости, поединечно и вкупно;
- постојните контроли и колку тие ефикасно ја намалуваат ранливоста.

Очекуван резултат: Веројатност за појава на безбедносно нарушување (квантитативно или квалитативно).

2.3.4. Ниво на ризикот

Опис на активноста: Нивото на ризик треба да се утврди за сите релевантни безбедносни нарушувања. Преку анализа на ризикот се доделуваат вредности за веројатноста и последиците од ризик. Овие вредности може да бидат квантитативни или квалитативни. Проценетиот ризик е комбинација на веројатноста за појава на безбедносно нарушување и неговите последици. Практично објаснување за секое ниво е дадено подолу:

НИСКО НИВО. Не се воочени активности што може да активираат даден ризик или истиот со контрамерки е сведен на најниско ниво, штонема да предизвика штети врз нормалното функционирање на работната организација. Загубата на доверливост, интегритет или достапност може да се очекува да имаат ограничено негативно влијание врз институционалните операции, средства или поединци.

(Нормално функционирање на институцијата. Алармните системи и безбедносните системи во институцијата се поставуваат на ниско обезбедување и ниска сензитивност).

СРЕДНО НИВО. Воочени се активности што може да активираат даден ризик или истиот со контрамерки не е сведен на најниско ниво со што би можел да предизвика штети, што би можеле да влијаат врз нормалното функционирање на работната организација. Загубата на доверливост, интегритет или достапност може да се очекува да има сериозно негативно влијание врз институционалните операции, средства или поединци.

(Зголемена е будноста на безбедносните органи во институцијата, алармните и безбедносните системи се поставуваат на највисоко ниво на заштита и се работи кон изработка на планови за работа во случај на високо ниво на загрозеност на институцијата согласно насоките на раководителот на институцијата).

ВИСОКО НИВО. Воочени се сериозни активности што се подготвени да активираат даден ризик што би можел да предизвика значителни штети, коишто може сериозно да влијаат врз функционирање на институцијата. Загубата на доверливост, интегритет или достапност може да се очекува да има катастрофално негативно влијание врз институционалните операции или поединци.

(Се прогласува во исклучителни случаи: војна, етнички конфликт, граѓанска војна, високи елементарни непогоди и друго).

Во согласност со состојбата на сите регистрирани ризици, се определува моменталната состојба на нивото на загрозеност. Со тоа при конечната изработка на процена на ризик на една институција, се прогласува и конечната состојба.

Очекуван резултат (Output): Листа на ризици со доделени вредности за нивото (Види: Додаток 4 - Пристап за процена на ризик за информатичка безбедноста).

2.4. Евалуација на ризикот

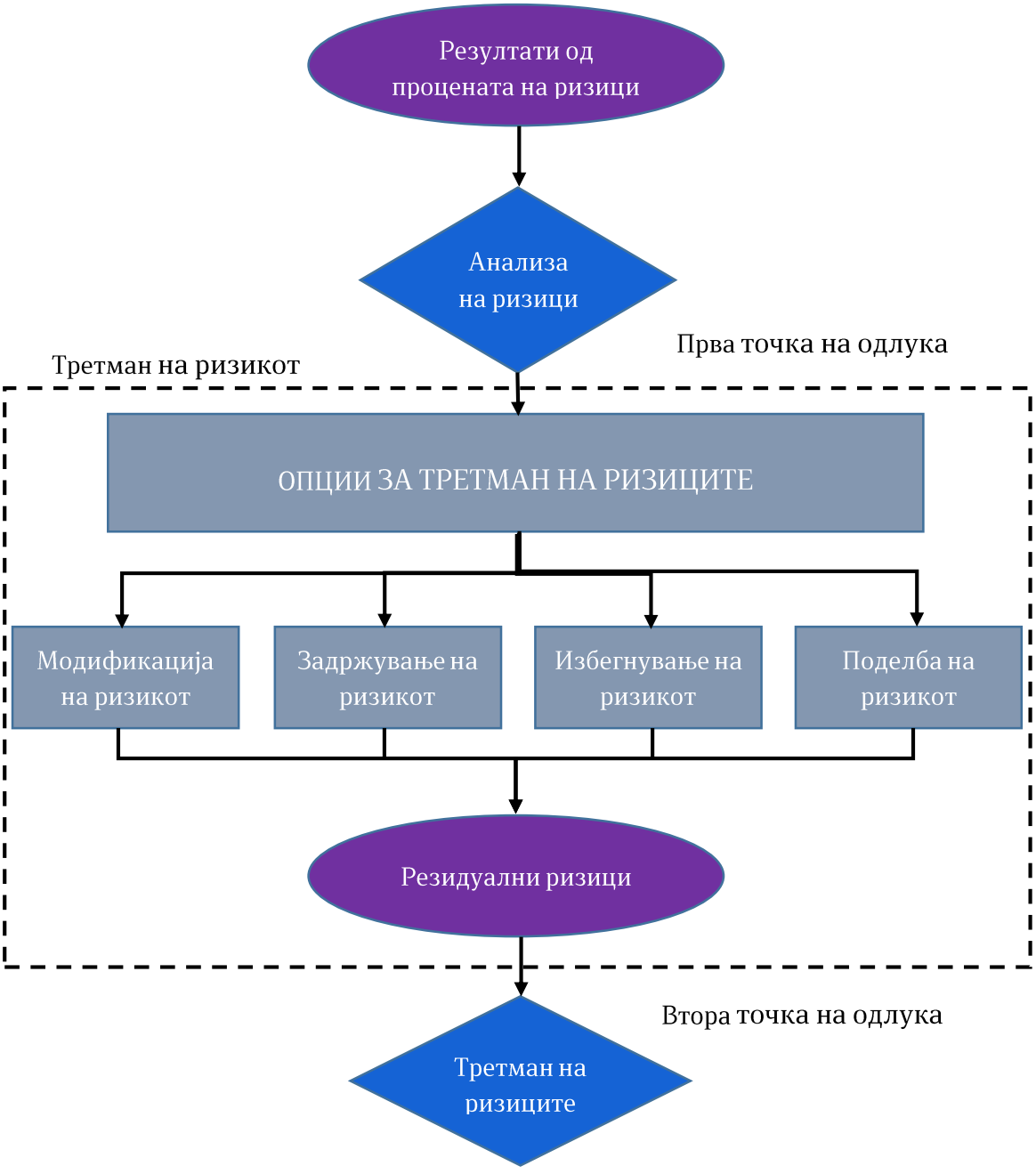
Опис на активноста: Нивото на ризикот треба да се спореди со критериумите за евалуација и прифатливост на ризикот. За да се евалуира ризикот, институциите треба да ги споредат проценетите ризици со критериумите за оценка на ризикот.

Критериуми за оценка на ризикот што се користат за да се направи одлука, треба да бидат во согласност со дефинираните надворешни и внатрешни услови на управување со ризикот врз безбедноста на информациите. Одлуките што се донесени во активноста за процена на ризикот се засноваат главно на прифатливото ниво на ризик. Сепак, последиците, веројатноста и степенот на доверба при идентификација на ризикот и анализата треба да се земат, исто така, во предвид. Агрегација на повеќе ниски или средни ризици може да резултира со многу повисок вкупен ризик и треба да се разгледа соодветно. Разгледувањето треба да содржи:

- безбедносно информатички својства: ако еден критериум не е релевантен за организацијата (на пример, губење на доверливост), тогаш сите ризици што влијаат на овој критериум не се релевантни и
- важноста на процесите или на активностите поддржани од страна на одредени средства или група на средства: ако процесот е утврден дека е со помала важност, ризиците поврзани со него треба да добијат пониско ниво на разгледување од ризиците што влијаат врз поважните процеси или активности.

Евалуацијата на ризикот го користи разбирањето за ризикот добиено со анализата на ризикот за да се донесат одлуки за понатамошни акции. Одлуките треба да содржат: дали треба да се преземе одредена активност и приоритети за третманот на ризикот, со оглед на проценетите нивоа на ризици.

Очекуван резултат: Листа на приоритетни ризици во согласност со критериумите за оценување на ризикот, во однос на безбедносните нарушувања што произлегуваат од тие ризици (Види: Додаток 4 - Пристап за процена на ризик за информатичка безбедноста).



Слика 1 – Дијаграм на активности при процесот на анализа на ризиците

3. Управување со безбедносен ризик

3.1. Дефиниција за управување со безбедносниот ризик

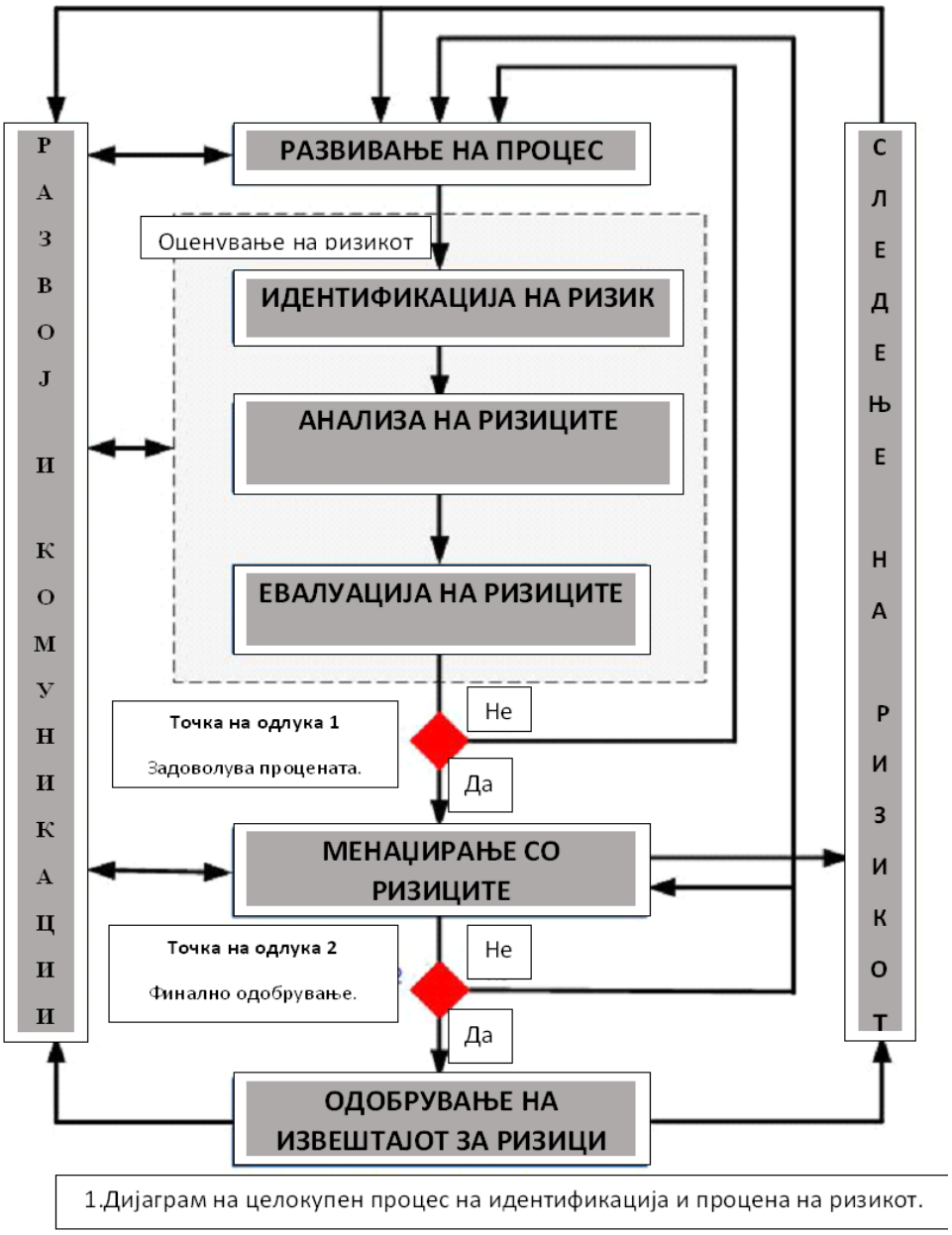
Управувањето со безбедносниот ризик претставува пронаоѓање на безбедносните контрамерки што се потребни за заштита на КИС и на ресурсите, базирани на заканите и на ранливостите, како и идентификација на опсегот и на целите на проценатa на безбедносниот ризик.

3.2. Фази на управување со безбедносниот ризик

Управувањето со безбедносниот ризик ги вклучува постапките на редукција, трансфер, елиминација, заобиколување и прифаќање. Управувањето вклучува процеси на планирање, организирање, избор, насока и контрола на ресурсите, со цел да се обезбеди и да се осигура дека ризикот е ставен во прифатливи граници. Управувањето со безбедносниот ризик ги содржи следните елементи:

- Селекција на превентивни мерки (идентификација на контрамерки, детерминација на неопходните контрамерки и компарација со веќе постојните, идентификација на контрамерките што веќе се инсталирани и оние што се препорачуваат).
- Прегледување и повторување на препорачаните контрамерки земајќи ги предвид минималните стандарди за заштита на класифицираните информации:
    - елиминација на ризикот (тотална елиминација на вистинските или потенцијалните слабости преку имплементација на контрамерките);
    - превенција на физичката или информатичката загуба (имплементација на контрамерките за да се спречи што е можно поголема загуба, имајќи предвид дека некои закани не може да се елиминираат во оперативниот процес);
    - ограничување на физичката и информатичката загуба (да се имплементираат контрамерките што би ги намалиле загубите на задоволително ниво);
    - прифатливост на физичките и информатичките загуби што би настанале, а не би влијаеле врз функционалноста на системот;

- развивање на извештајот за управување на безбедносниот ризик што се состои од опис на контрамерки што се имплементираат во работен план и опишувањето на резидуалниот ризик и
- испитување на безбедносните процедури на база на периоди.



Слика 2 – Дијаграм на целокупен процес на идентификација и процена на ризикот

3.3. Вреднување на ризиците и изработка на матрици

За секоја категорија на ризик се дава одреден опсег со оценки којшто потоа се сумира и дава математички резултат што го дава степенот на градација на мерната единица. За да се добие целосен увид на степенот на загрозување се изработуваат квалитативни матрици во коишто веројатноста за случување на заканата - ризикот на дводимензионална скала на вредности е вкрстена со ударот што би се случил доколку некој одреден ризик се материјализира. Со класификација и на ударот и на веројатноста за случување на ризикот на скала од „многу ниско“ до „многу високо“, т.е со позиционирање на секој ризик на скалата согласно неговата релеватност, се одредува ризикот за безбедноста. Иако ова е субјективна процена, степенот на одредување на ранливоста е доверлив и непристрасен процес.

Пример:

1. Акредитирани компјутерски системи.....од 1 до 4
2. Соодветни простории.....од 1 до 4
3. Објекти – згради.....од 1 до 5, без 4
4. Пристап кон 1, 2 и 3.....од 1 до 4
   - контрола на влез и излез..... 3 или 1
5. Администраторски системи.....од 1 до 5
   - - администраторски лозинки.....од 1 до 4
6. Лиценциран софтвер.....од 1 до 4
   - - конфигурација на хардвер.....од 0 до 1
   - - конфигурација на софтвер.....од 0 до 1
   - - кориснички лозинки.....од 0 до 1
   - - кориснички права и дозволи.....од 0 до 1
   - - CCTV камери.....од 0 до 1
7. Сумирање на резултатите од точка 1 до точка 6

Сумираното резултат преставува математички број што дава споредбена мерка за задоволувачкиот степен на оценуваниот систем.

Подолу во табела е дадена пример на матрица земајќи ја предвид веројатноста од можноста да се случи безбедносно нарушување. Веројатноста е дадена преку третирање на заканата и ранливоста со

одредена веројатност односниот настан да се материјализира. Резултатот на ризикот е мерен на скала од 0 до 8.

Веројатност да се случи инцидент / Последици	Многу мала	Мала	Средна	Голема	Многу голема
Многу мали	0	1	2	3	4
Мали	1	2	3	4	5
Средни	2	3	4	5	6
Големи	3	4	5	6	7
Многу големи	4	5	6	7	8

На пример:

- Низок ризик:.....0-2;
- Среден ризик:.....3-5;
- Висок ризик: .....6-8.

3.4. Документирање

Резултатот од проценатa на безбедносниот ризик преку почитување на минимум стандардите на заштитните мерки треба да се документира во „*Процена на ризик за комуникациско-информатички системи*”. Проценатa треба да ги содржи следните компоненти:

- лелите и задачите на проценатa на безбедносниот ризик;
- состојба на безбедносните задачи (цели) на организацијата во смисла на доверливост, интегритет и слобода на проток;
- проценка на резидуалниот ризик за да биде прифатен во процесот;
- листа на нови и постојни протективни мерки (надградување на постојните);
- опис на заштитните мерки и нивна практична функционалност и
- детаљен работен план за имплементација на заштитните мерки, безбедносна програма за подобрување, како и опис на мониторинг на прогресот на имплементација на самата програма.

Начинот и постапката на процесот на изработка на проценатa е даден во Додаток 5 – Дијаграм за процесот на одвивање на анализата на ризик.

4. Заклучок и идни согледувања

Нивото на заштита на безбедносниот систем на една земја зависи од постоењето и соодветното имплементирање процедури за процена на ризик. Поверојатно е државните и приватните чинители на безбедносниот систем и на критичната инфраструктура на една земја да се вклучат во заштитата на националниот безбедносен систем, доколку се изготви сеопфатна процена на ризик. Следејќи ја структурата на меѓународниот стандард за процена на ризик ISO/IEC 27005:2011 и елементите што овој стандард ги вклучува, оваа методологија за процена на ризик за информатичката безбедност е последица од утврдената празнина во Република Македонија за дополнување на правната рамка којашто ја покрива информатичката безбедност, а конкретно рамката за процена на ризик. Тековните процени на ризик, имплементирани главно на микро-организациско ниво, ги покриваат вообичаено физичките аспекти на безбедноста, без притоа да го земат предвид значењето на комуникациско-информатичките системи. Отсуството на сеопфатна процена на ризик за информатичка безбедност го намалува нивото на безбедносна свест и ги забавува механизмите за реакција при потенцијални закани. Целосно елаборирајќи ги трите најважни компоненти на проценатa на ризик: идентификација на ризик, анализа на ризик и евалуација на ризик, оваа методологија за процена на ризик ја трасира траекторијата на изработка на процена за ризик и претставува дополнителен инструмент којшто помага да се процени подготвеноста на една институција/организација во справувањето со безбедносните закани. Од друга страна, со помош на управувањето со ризик, што е детално објаснето во последниот дел од оваа методологија, на најпрактичен и илустративен начин е објаснета процедурата за изработка на процена на ризик.

Секоја институција/организација е одговорна за имплементација на оперативно-безбедносните процедури, а со тоа и потребата да се развие процена на ризик за информатичка безбедност. Персоналот задолжен за идентификација, анализа и евалуација на безбедносните ризици е директно одговорен за имплементација на проценатa на ризик додека менаџментот на организацијата е директно вклучен и одговорен за процесот на управување со безбедносниот ризик. Во согласност со потребата за континуирана верификација и тестирање на имплементацијата на проценатa за ризик како и во насока на антиципирање на идните предизивици во делот на информатичката безбедност се утврдуваат следните главни активности и иницијативи за намалување на заканите и пропустите: креирање

национална проценка на ризик, детерминирање на критично-информацискатa инфраструктура и спроведување на режимот на акредитација околу нив, промовирање на употребата на проверени софтверски производи, приоритизирање на истражувачките и развојни активности за одржување на националните безбедносни процедури, перманентна надоградба на проценатa во согласност со ново вградените системи и појавата на нови закани, подобрување на безбедноста на интернет протоколи, изработка на акциски планови за имплементација на проценатa на ризик, идентификување авторитет што ќе го мониторира процесот на имплеменатација, ќе ги евалуира резултатите и ќе предлага подобрувања и унапредувања на постојните. Оттука, од особена важност е да се истакне дека изработката на проценатa за ризик не е процес што ќе се заврши еднаш и ќе трае засекогаш. Напротив, проценатa за безбедносен ризик се повторува, се прегледува и се надградува.

Оваа методологија за изработка на процена на ризик, претставува уште еден чекор кон зајакнување на регулаторната рамка од областа на информатичката безбедност во Република Македонија.