ДОДАТОК 4

ПРИСТАП ЗА ПРОЦЕНА НА РИЗИК ЗА ИНФОРМАТИЧКА БЕЗБЕДНОСТ

1. Детални информации за процена на безбедносен ризик

Процесот на процена на безбедносен ризик подразбира подетална идентификација на вредноста на ресурсите, процена на заканите за овие ресурси, како и процена на ранливостите. Резултатите од овие активности потоа се користат за процена на ризикот и за идентификување на мерките за справување со ризикот.

Завршната фаза при процена на ризик на безбедност на информации е процена на целокупните ризици што всушност претставува тема на овој додаток.

Многу методи вклучуваат користење табели како и комбинација од субјективни и емпириски мерки. Важно е да се напомене дека организацијата го користи оној метод за којшто смета дека е најпогоден, којшто е релевантен за користење и којшто може да продуцира повторливи резултати. Неколку примери на техники базирани на табели се дадени подолу.

Следниве примери користат броеви за да опишат квалитативни процени. Корисниците на овие методи треба да имаат предвид дека изведувањето на понатамошни математички операции може да биде невалидно доколку броевите коишто се квалитативни резултати се изведени со помош на квалитативни методи за процена на ризик.

1.1. Пример 1: Матрица со претходно дефинирани вредности

Во методите за процена на ризик од овој тип реалните или предложените физички ресурси се вреднуваат во однос на трошоците за замена или реконструкција (на пример: квантитативни мерења). Овие трошоци потоа се пренесуваат на истата квалитативна скала којашто се користи за информациите (види подолу). Реалните или предложените софтверски ресурси се вреднуваат на ист начин како и физичките ресурси со помош на идентификување на трошоците за набавка или реконструкција коишто потоа се пренесуваат на истата квалитативна скала што се користи за информациите.

Вредностите на ресурсите, како и степенот на заканата и ранливост, соодветни за секој вид на последица се вкрстуваат како во матрицата што е прикажана подолу со цел да се идентификуваат, за секоја комбинација,

соодветната величина на ризик на скала од 0 до 8. Вредностите се поставени во матрицата на структуриран начин. Во продолжение е даден еден пример:

	Веројатност за реализација – закана	Ниско ниво			Средно ниво			Високо ниво		
	Леснотија на злоупотреба	н	с	в	н	с	в	н	с	в
Вредност на ресурсите	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Табела 1

За секој ресурс се земаат предвид релевантните ранливости и нивните соодветни закани. Ако постои ранливост без соодветна закана или закана без соодветна ранливост, тогаш во моментот не постои ризик (но треба да се внимава во случај на промена на оваа ситуација). Соодветниот ред во матрицата се идентификува по вредност на ресурсите, и соодветната колона е идентификувана по веројатноста за појава на заканата и леснотија на злоупотреба. На пример, ако ресурсот има вредност 3, заканата е **висока,** а ранливоста **ниска**, величината на ризикот изнесува 5. Да претпоставиме за промена, на пример, дека еден ресурс има вредност 2, нивото на заканата е ниска и леснотија на злоупотреба е висока, тогаш величината на ризикот е 4. Големината на матрицата, во поглед на бројот на категории на веројатности на заканите, категориите за леснотија на злоупотреба и бројот на категориите за вреднување на ресурсите може да се приспособи според потребите на организацијата. Дополнителни колони и редови, ќе бараат дополнителни величини на ризик. Вредноста на овој пристап е во рангирањето на ризиците што треба да се отстранат.

Слична матрица, како што е прикажана во Табела 2, произлегува од разгледувањето на можноста на сценарио за инцидент, претставено во однос на проценетото влијание од работењето. Веројатноста за сценарио за инцидент е прикажана со закана на искористување на ранливост со одредена веројатност. Произлезениот ризик се мери на скала од 0 до 8 што може да се процени во однос на критериуми за прифаќање на ризик. Оваа скала на ризик, исто така, може да биде прикажана едноставно како целокупно рангирање на ризик, како на пример:

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

	Веројатност за сценарио на инцидент	Многу ниско (малку веројатно)	Ниско (неверојатно)	Средно (можно)	Високо (веројатно)	Многу високо (често)
Влијание врз работењето	Многу ниско	0	1	2	3	4
	Ниско	1	2	3	4	5
	Средно	2	3	4	5	6
	Високо	3	4	5	6	7
	Многу високо	4	5	6	7	8

Табела 2

1.2. Пример 2: Рангирање закани според величини на ризик

Матрицата што е прикажана во Табела 3 може да се користи да се поврзат факторите на последици (вредност на ресурсите) и веројатноста за реализација на закана (земајќи ги предвид аспектите на ранливоста). Првиот чекор е да се оценат последиците (вредноста на ресурсите) на претходно дефинирана скала, на пример од 1 до 5, на секој ресурс којшто е под закана (колона б во Табелата). Втор чекор е да се оцени веројатноста за појава на закана на претходно дефинирана скала, на пример од 1 до 5, на секоја закана (колона Ц во табелата). Третиот чекор е да се пресмета величината на ризикот преку множење на колоните Б и Ц (Б х Ц). На крајот заканите се подредуваат според редослед на односните величини на ризикот. Треба да се има предвид дека во овој пример 1 е земен како најмала последица и најниска веројатност на појава на ризик.

Опишувач на закана (а)	Вредност на (средства) последици (б)	Веројатност за појава на заканата (ц)	Величина на ризик (д)	Рангирање на заканата (е)
Закана А	5	2	10	2
Закана Б	2	4	8	3
Закана Ц	3	5	15	1
Закана Д	1	3	3	5
Закана Е	4	1	4	4
Закана Ф	2	4	8	3

Табела 3

1.3. Пример 3: Процена на вредноста за веројатност и можните последици од ризикот

Во овој пример, акцентот е ставен на последиците од инциденти во информатичката безбедност (односно сценарија со инциденти) и на одредувањето на кои системи треба да им се даде приоритет. Ова се прави со процена на две вредности за секој ресурс и ризик, што во комбинација ќе одредат резултат за секој ресурс. Кога ќе се сумираат сите резултати за системот, тогаш се одредува величината на ризик за тој систем.

Прво, се доделува вредност на секој ресурс. Оваа вредност се однесува на можните штетни последици што можат да настанат доколку ресурсот е под закана.

Следно, се проценува вредноста на веројатноста за случување на заканата. Ова се проценува со комбинација на веројатноста за случување на заканата и леснотијата на злоупотреба на ранливоста. Табела 4 ја прикажува веројатноста на едно сценарио на инцидент.

Веројатност за закана	Ниско			Средно			Високо		
Степен на ранливост	Н	С	В	Н	С	В	Н	С	В
Вредност на веројатност на сценарио за инцидент	0	1	2	1	2	3	2	3	4

Табела 4

Следно, вредност на ресурс/закана се доделува со изнаоѓање на пресекот на вредноста на ресурсот и вредноста на веројатноста за случување на заканата што е дадено во Табела 5. Добиените вредности за ресурсот/заканата се собираат за да се добие вкупен резултат за ресурсот. Овој резултат може да се користи за да се одвојат ресурсите што се дел од системот.

Вредност на ресурсите	0	1	2	3	4
Вредност на веројатност					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Табела 5

Последен чекор е да се соберат сите вкупни вредности за ресурсите на системот, формирајќи на тој начин системски резултат. Ова може да се користи да се направи разлика помеѓу системите и да се утврди на кој систем за заштита треба да му се даде приоритет.

Во следните примери сите вредности се избрани по случаен избор.

Да претпоставиме дека системот има три ресурси A1, A2 и A3. Исто така, да претпоставиме дека постојат две закани T1 и T2 што се однесуваат на системот C. Нека вредноста за A1 биде 3, а на сличен начин вредноста на ресурсот A2 нека биде 2 и вредноста на ресурсот A3 нека биде 4.

Ако за A1 и T1 веројатноста дека заканата е ниска и леснотијата на злоупотреба на ранливоста е средна, тогаш вредноста на веројатноста е 1 (види Табела 4).

Вредноста на ресурсот/заканата A1/T1 може да се изведе од Табелата 5 како збир на вредноста на ресурсот 3 и вредноста на веројатноста 1, односно 4.

Слично, за A1/T2 веројатноста дека заканата е средна и леснотијата на злоупотреба на ранливост е на високо ниво, за A1/T2 се добива вредност 6.

Сега вкупниот збир на ресурсот A1 T може да се пресмета, односно тоа е 10. Вкупен резултат на ресурсите се пресметува за секој ресурс и за заканите коишто се апликативни. Вкупниот резултат на системот се пресметува со собирање на A1T + A2T +A3T кои треба да дадат CT.

Горенаведениот пример се однесува на информатичките системи. Сепак, сличен пристап може да се примени и на работните процеси.