Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

Утвърдени със Заповед на
председателя на ДАЕУ
№ ДАЕУ-1125/24.01.2020 г.

МЕТОДИКА И ПРАВИЛА ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА ЗА СЪОТВЕТСТВИЕ С МЕРКИТЕ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, ОПРЕДЕЛЕНИ С НАРЕДБАТА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

гр. София, 2020г.

1000 гр. София, ул. "Ген. Й. В. Гурко" № 6,
тел.: (+359 2) 949 20 40, факс:(+359 2) 949 21 58
www.e-gov.bg, e-mail: mail@e-gov.bg

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

1. Тази Методика урежда начина за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени в Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), наричана за краткост по-нататък „оценка“.

2. На оценяване подлежат всички субекти, посочени в чл. 1, ал. 1 от НМИМИС.

3. При извършване на оценка се спазват принципите на законосъобразност, обективност, ефективност, безпристрастност, професионализъм, независимост и конфиденциалност.

Списък на извършените оценки за мрежова и информационна сигурност

4. Всеки Национален компетентен орган по чл.16 от Закона за киберсигурност създава списък на извършените по настоящата методика оценки.

5. Публичната информация от списъка по т. 7.1 може да се публикува на интернет страницата на административния орган към който е създаден съответния Национален компетентен орган веднъж годишно. Националният компетентен орган към Държавна агенция „Електронно управление“ задължително публикува публичната информация на портала за мрежова и информационна сигурност – govcert.bg.

6. Списъка се попълва с данни от анкетата от Приложение №1, попълнени от субектите по чл. 1, ал. 1 от НМИМИС.

7. Списъкът съдържа най-малко:

7.1. публична информация

7.1.1. дата на извършване на оценката;

7.1.2. наименование на оценявания субект по чл. 1, ал. 1 от НМИМИС.

7.2 непублична информация

7.2.1. всички въпроси от Приложение №1 и съответните отговори;

7.2.2. дадени препоръки (ако има такива);

7.2.3. забележки (ако има такива).

Глава втора
ПРАВИЛА ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА ЗА СЪОТВЕТСТВИЕ С МЕРКИТЕ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, ОПРЕДЕЛЕНИ С НАРЕДБАТА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

8. Оценяването се извършва на база попълнените от оценявания отговори на въпросите в анкетата от Приложение №1.

9. На субектите по чл. 1, ал. 1 от НМИМИС, които попадат в годишната програма по чл. 36, ал. 3 от НМИМИС, приоритетно се извършва оценка за съответствие с мерките за мрежова и информационна сигурност по настоящата методика.

10. На субектите по чл. 1, ал. 1 от НМИМИС, които не попадат в годишната програма по чл. 36, ал. 3 от НМИМИС, се извършва оценка за съответствие с мерките за мрежова и информационна сигурност по настоящата методика съобразно възможностите и ресурсите на съответния Национален компетентен орган.

11. Резултатите от попълнените анкети може да се предоставят на съответните компетентни органи за извършване на проверка.

Глава трета
МЕТОДИКА ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА ЗА СЪОТВЕТСТВИЕ С МЕРКИТЕ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, ОПРЕДЕЛЕНИ С НАРЕДБАТА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Процес на извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с НМИМИС

12. Мрежовата и информационната сигурност се оценява по отношение спазване на мерките, посочени в Глава втора на НМИМИС.

13. Анкетата от Приложение №1 се изпраща с писмо до ръководителя на субекта по чл. 1, ал. 1 от НМИМИС за попълване. След попълване на отговорите, анкетата се класифицира с ниво TLP-AMBER съгласно НМИМИС.

14. Оценявания субект по чл. 1, ал. 1 от НМИМИС предоставя обратно попълнена анкета в срок до един месец след нейното получаване.

15. За да се установи верността на попълнени отговори на въпроси от анкетата, за съответствие с мерките на Глава втора от НМИМИС, упълномощени служители на Националния компетентен орган може да извършат сканиране за уязвимости на информационни ресурси, за което проверявания субект по чл. 1, ал. 1 от НМИМИС се уведомява предварително. Резултатите от сканирането се нанасят в доклад заедно с всички събрани доказателства от сканирането.

Указания за попълване на анкетата по Приложение №1 и формиране на оценка

16. Единствените валидни форми за отговор на въпросите от анкетата са: “да”; ”не” и “неприложимо”. Всички въпроси, на които не е отговорено с една от гореизброените форми се считат за отговор със стойност “не”.

17. Стойностите и различните променливи във формулата за изчисление на оценката са както следва:

Стойности на отговорите:

“да” – изискванията на въпроса са цялостно изпълнени;

“не” – изискванията на въпроса не са изпълнени цялостно или частично;

“неприложимо” – изискванията на въпроса не се отнасят за оценявания субект;

Променливи:

a= Брой на всички възможни отговори в анкетата минус броят на отговорите, на които е отговорено с “неприложимо”;

y= брой отговори, със стойност “да”

f= оценка

18. Формула:

(y/a).100 = f%

Сканиране за уязвимости на информационни ресурси

19. Сканиране за уязвимости се извършва само за информационни ресурси. За информационен ресурс за целите на настоящата методика се счита ресурс, който отговаря на следните условия:

19.1. Има реален IP адрес, който е достъпен през Интернет;

19.2. Е поне едно от изброените:

а. уеб сайт;

б. уеб порт;

в. уеб платформа;

г. уеб приложение;

д. сървър;

е. пощенски сървър;

ж. електронен регистър.

20. Сканирането за уязвимости включва следните стъпки:

20.1. сканиране за уязвимости в информационен ресурс посредством наличните инструменти;

20.2. събиране и документиране на информацията, получена посредством сканирането за уязвимости в първа стъпка;

20.3. оценка и анализ на събраната информация;

20.4. извършване на проверка за съответствие между резултатите от анализираната информация и контролите в НМИМИС;

20.5. Изготвяне на доклад, който да отрази това съответствие (несъответствие).

21. Сканирането за уязвимости се инициира със заповед , като в заповедта задължително се посочват:

21.1. периода, в който трябва да бъде извършено сканирането;

21.2. информационни ресурси , които ще бъдат сканирани;

21.3. идентификационни данни на субекта, чийто информационни ресурси ще бъдат сканирани;

21.4. имената на служителите, които ще извършат сканирането.

22. Сканиране за уязвимости се извършва от външна за оценяваните мрежа, като целта е да се провери съответствието с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност. Когато информационен ресурс е недостъпен от външни мрежи, сканиране не се извършва.

23. Ръководителя на субекта, чиито информационни ресурси ще бъдат сканирани се уведомява за периода, през който ще бъде извършено сканирането най-малко 3 (три) дни преди началото на сканирането.

24. Резултатите от сканирането се нанасят в доклад по образец, посочен в Приложение №2. Като приложение към доклада се представят всички събрани доказателства от сканирането.

25. Копие от доклада, заедно с всички събрани доказателства се предоставя на съответната структура на Националния компетентен орган за извършване на контрол.

26. Сканирането за уязвимости задължително се извършва от поне двама служители.

27. Възможно е да бъдат привличани и външни експерти за извършване на сканирането.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. Методиката се изготвя и приема на основание чл. 12, т. 7 от Закона за киберсигурност (Обн. ДВ. бр. 94 от 13 ноември 2018г.).