20261392033

МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

Врз основа на член 23 став (6) од Законот за безбедност на мрежни и информациски системи (*) („Службен весник на Република Северна Македонија“ бр. 135/25), министерот за дигитална трансформација донесе

МЕТОДОЛОГИЈА ЗА СПРОВЕДУВАЊЕ НА АНАЛИЗА НА РИЗИК ЗАРАДИ ПРИОРИТИЗАЦИЈА НА ЗАДАЧИТЕ НА ТИМОТ ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ ЗА ОРГАНИТЕ НА ИЗВРШНАТА ВЛАСТ

Предмет

Член 1

Со оваа методологија се пропишува спроведувањето на анализата на ризик заради приоритизирање на задачите на Тимот за одговор на компјутерски инциденти за органите на извршната власт во рамките на Министерството за дигитална трансформација (во натамошниот текст: MKD-GOV-CSIRT).

Анализа на ризик

Член 2

Анализата на ризик заради приоритизирање на задачите ја спроведува MKD-GOV-CSIRT и истовремено треба да извршува повеќе задачи.

Анализата на ризик заради приоритизирање на задачите на MKD-GOV-CSIRT се спроведува врз основа на:

- вид на субјектот и
- вид на работните задачи.

Анализата на ризик ја подготвува раководителот на MKD-GOV-CSIRT.

Врз основа на спроведената анализа на ризик се подготвува План со приоритетни задачи со временска рамка заради ефикасно извршување на сите работни задачи.

Вид на субјект

Член 3

Врз основа на „вид на субјект“ се врши анализа врз основа на видот на субјекти во однос на тоа дали субјектот кон кој MKD-GOV-CSIRT ги реализира работните задачи е суштински или важен.

Приоритет имаат суштинските субјекти.

Вид на работни задачи

Член 4

Врз основа на „вид на работни задачи“ се врши анализа врз основа на видот на работните задачи врз основа на тоа дали работните задачи се насочени кон справување на веќе постоечки сајбер безбедносен инцидент, намалување на ризиците од постоечка сајбер безбедносна закана или пак имаат превентивен карактер.

Приоритет имаат работните задачи насочени кон справување на веќе постоечки сајбер безбедносен инцидент, потоа следуваат задачите поврзани со намалување на ризиците од постоечка сајбер безбедносна закана и на крај се задачите од превентивен карактер (следење и анализирање на ранливости, доставување на рани предупредувања, собирање и анализа на форензички податоци, проактивно скенирање на мрежни и информатички системи на суштински и важни субјекти, учество во мрежата на тимови за справување со компјутерски инциденти, градење на капацитети и сл.).

Во случај на повеќе работни задачи од превентивен карактер, приоритет имаат тие кои се директно поврзани со спречување на сајбер безбедносните инциденти.

Влегување во сила

Член 5

Оваа методологија влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Северна Македонија”.

Бр. 10-1456/1
24 јуни 2026 година
Скопје

Министер за дигитална
трансформација,
Стефан Андоновски с.р.