Република Северна Македонија

Министерство за дигитална трансформација

МЕТОДОЛОГИЈА ЗА ПОБЛИСКИТЕ КРИТЕРИУМИ, КАКО И ПРАГОТ НА ОПРЕДЕЛУВАЊЕ НА ОБИЧНИ И ЗНАЧАЈНИ САЈБЕР БЕЗБЕДНОСНИ ИНЦИДЕНТИ

ОПШТИ ОДРЕДБИ

Цел

Член 1

Оваа Методологија ги пропишува поблиските критериуми, како и прагот на определување на обични и значајни сајбер безбедносни инциденти за Владата, министерствата, самостојните органи на државната управа, органите на државната управа вклучувајќи ги управните организации, општините, општините во градот Скопје и градот Скопје.

Намена

Член 2

Методологијата е наменета за брза идентификација и класификација на сајбер безбедносни инциденти, носење на одлука за ескалација, приоретизирање во фаза на опоравување од сајбер безбедносни инциденти како и конзистентно известување и анализа на настанатите сајбер безбедносни инциденти.

КЛАСИФИКАЦИЈА НА САЈБЕР БЕЗБЕДНОСНИ ИНЦИДЕНТИ

Класификација

Член 3

Сајбер- безбедносните инциденти се класифицираат во следните категории:

Категорија 1	**Инциденти со компромитација**
Категорија 2	Инциденти со нарушување на услуги
Категорија 3	Инциденти со закана или слабост

Инциденти со компромитација

Член 4

Инциденти со компромитација се настани кај кои постои неовластен пристап, компромитација на системи, мрежи или апликации и/или нарушување на доверливоста и/или интегритетот на податоците:

Основни карактеристики	• Неовластен пристап • Компромитација на ИКТ ресурси • Нарушување на доверливост • Нарушување на интегритет

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

Опфат	• Злонамерен софтвер (ransomware, spyware, backdoor) • Неовластен пристап или преземање кориснички сметки • Истекување или кражба на податоци • Искористување на ранливости • Внатрешни (insider) инциденти • Supply chain компромитации

Инциденти со нарушување на услуги

Член 5

Инциденти со нарушување на услуги се настани кои доведуваат до делумен или целосен прекин на ИКТ услуги, деградација на перформанси или онеспособување на системи или инфраструктура:

Основни карактеристики	• Прекин на услуги • Намалени перформанси • Онеспособени системи
Опфат	• DoS/DDoS напади • Ransomware со блокирање на системи • Саботажа на ИКТ ресурси • Прекини предизвикани од безбедносен настан

Инциденти со закана или слабост

Член 6

Инциденти со закана или слабост се настани кои не резултирале со директна компромитација или прекин, но претставуваат реален ризик за безбедноста:

Основни карактеристики	Потенцијален безбедносен ризик без остварена штета
Опфат	• Phishing и други облици на социјален инженеринг • Идентификувани технички ранливости • Неправилни конфигурации • Прекршување на безбедносни политики • Физички безбедносни слабости

КРИТЕРИУМИ ЗА ПРОЦЕНКА

Поблиски критериуми за проценка на сајбер безбедносни инциденти

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

Член 7

Проценката на сајбер безбедносните инциденти се врши врз основа на следните поблиски критериуми, независно од нивната класификација и тоа дали инцидентот има:

Критериум	Нивоа / Опис
1. Влијание врз доверливост, интегритет и достапност (CIA)	• Нема влијание • Ограничено / локално влијание • Значајно влијание • Сериозно или целосно нарушување
2. Опфат и распространетост	• Еден систем или корисник • Повеќе системи • Повеќе организациски единици • Повеќе институции / прекугранично
3. Намерност и сложеност	• Случаен / ненамерен настан • Едноставен, ненасочен напад • Насочен напад • Координиран или напреден напад
4. Времетраење и опоравување	• Краткотраен (< 1 час) • Среден (1 – 4 часа) • Долготраен (4 – 24 часа) • Потреба од надворешна или специјализирана поддршка (> 24 часа)
5. Правно, регулаторно и репутациско влијание	• Нема обврска за известување • Внатрешно известување • Национална обврска за известување на MKD-GOV-CSIRT • Меѓународно влијание / сериозен репутациски ризик

Праг за определување на значајност

Член 8

Согласно значајноста сајбер безбедносните инциденти можат да се поделат на 2 (два) вида и тоа:

Тип на инцидент	Целосни критериуми
Обичен сајбер безбедносен инцидент	• Ниско или ограничено влијание • Зафатен мал број системи или корисници • Нема истекување чувствителни податоци • Нема значајно нарушување на услуги

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

	• Решлив со стандардни оперативни процедури • Нема законска обврска за надворешно известување
Значаен сајбер безбедносен инцидент	• Сериозно нарушување на доверливост, интегритет или достапност • Компромитација или истекување на чувствителни, лични или класифицирани податоци • Прекин или значајно нарушување на јавни или критични услуги • Зафатени повеќе системи или институции • Сомнеж за координиран или напреден напад • Потреба од ескалација до национален MKD-GOV-CSIRT • Законска или меѓународна обврска за известување • Потенцијал за широко повторување или системски ризик

ЗАВРШНИ ОДРЕДБИ

Влегување во сила

Член 9

Оваа Методологија влегува во сила од денот на објавување во „Службен весник на Република Северна Македонија“

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски” бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk