Во согласност со член 33 став (12) од Законот за безбедност на мрежните и информациските системи (*) ("Службен весник на Република Северна Македонија" бр. 135/25), министерот за дигитална трансформација донесе

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

Предмет
Член 1

Со оваа методологија се пропишуваат поблиските критериуми, како и прагот за утврдување на обични и значајни сајбер безбедносни инциденти во Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации и општините, општините во градот Скопје и градот Скопје.

Поблиски критериуми за определување на обични и значајни сајбер безбедносни инциденти
Член 2

Прагот за определување на обичните и значајните сајбер безбедносни инциденти во Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации и општините, општините во градот Скопје и градот Скопје се врши врз основа на следните критериуми:

- Системски ризик;
- Прекугранично влијание;
- Влијание врз јавната безбедност, безбедноста или здравјето на луѓето;
- Специфично национално значење;
- Злоупотребата на податоци; и
- Материјална штета.

Системски ризик
Член 3

(1) Со критериумот „системски ризик“ се проценува можноста за нарушување на испораката на услуги во истиот сектор на кој припаѓа субјектот или во други поврзани сектори.

(2) Ако нарушувањето на испораката на услугата би предизвикало умерен ризик, односно нарушување во истиот сектор на кој припаѓа субјектот и/или умерено влијание врз други сектори, тоа е обичен сајбер безбедносен инцидент.

(3) Ако нарушувањето на испораката на услугата би предизвикало значителен системски ризик, предизвикувајќи широко распространети нарушувања на услугите во истиот сектор на кој припаѓа субјектот и/или во повеќе критични национални сектори, тоа е значаен инцидент на сајбер безбедност.

Прекугранично влијание

Член 4

(1) Со критериумот „прекугранично влијание“ се проценува можноста за нарушување на испораката на услуги кое ќе предизвика последици што се протегаат надвор од националните граници. Проценката ја зема предвид меѓусебната поврзаност на услугата на субјектот во меѓународната економија.

(2) Ако нарушувањето на испораката на услугата би предизвикало умерен ризик кој би довел до умерено прекугранично влијание, тоа е обичен сајбер безбедносен инцидент.

(3) Ако нарушувањето на испораката на услугата би предизвикало значителен системски ризик, предизвикувајќи широко распространети нарушувања во повеќе критични сектори на меѓународно ниво, тоа е сајбер безбедносен значаен инцидент.

Влијание врз јавната безбедност, безбедноста или здравјето на луѓето

Член 5

(1) Со критериумот „влијание врз јавната безбедност, безбедноста или здравјето на луѓето“ се проценуваат директните и индиректните последици од прекинот на испораката на услугата врз јавната безбедност, безбедноста или здравјето на луѓето.

(2) Ако нарушувањето на испораката на услугата претставува значителна закана за јавната безбедност, безбедноста или здравјето на луѓето, потенцијално влијаејќи на поголем број на граѓани, но без директна закана по јавната безбедност, безбедноста или здравјето на луѓето, тоа е обичен сајбер безбедносен инцидент.

(3) Ако нарушувањето на испораката на услугата би претставувало непосредна, широко распространета и директна закана за јавната безбедност, безбедноста или здравјето на луѓето, тоа е значаен инцидент во сајбер безбедноста.

Специфично национално значење

Член 6

(1) Со критериумот „специфично национално значење“ се проценува единствената и незаменлива улога на субјектот и услугите кои ги испорачува во одреден сектор или на национално ниво.

(2) Ако услугите кои ги испорачува субјектот се суштински за голем дел од секторот, и прекинот во нивната испорака сериозно би ја нарушил функционалноста на секторот на национално ниво, тоа е обичен сајбер безбедносен инцидент.

(3) Ако услугите кои ги испорачува субјектот се суштински на национално ниво или за други меѓузависни сектори, тоа е значаен сајбер безбедносен инцидент.

Злоупотреба на податоци

Член 7

(1) Со критериумот „злоупотреба на податоци“ се проценува можноста сајбер безбедносниот инцидент да ги загрози личните или класифицираните податоци.

(2) Ако инцидентот не ги загрозува посебните категории на лични податоци на граѓаните или класифицираните податоци, тоа е обичен сајбер безбедносен инцидент.

(3) Ако инцидентот ги загрозува посебните категории на лични податоци на граѓаните или класифицираните податоци, тоа е значаен сајбер безбедносен инцидент.

Материјална штета
Член 8

(1) Со критериумот „материјална штета“ се проценува можноста сајбер безбедносниот инцидент да предизвика значајна материјална штета.

(2) Ако сајбер безбедносниот инцидент не предизвика значајна финансиска штета (помалку од 250 просечни плати во земјата во моментот на инцидентот), се работи за обичен сајбер безбедносен инцидент.

(3) Ако сајбер безбедносниот инцидент предизвика значајна материјална штета (повеќе од 250 просечни плати во земјата во моментот на инцидентот), тоа е значаен сајбер безбедносни инцидент.

Стапување на сила
Член 8

Оваа методологија влегува во сила со денот на објавување на веб страната на Министерството за дигитална трансформација.

Бр.
година 2026
Скопје

Министер за дигитална трансформација,
Стефан Андоновски