20261412051

МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

Врз основа на член 22 став (3) од Законот за безбедност на мрежни и информациски системи (*) („Службен весник на Република Северна Македонија“ бр. 135/25), министерот за дигитална трансформација донесе

ПРАВИЛНИК ЗА НАЧИНОТ НА ПРИЈАВА И ПОСТАПУВАЊЕ ПО ПРИЈАВЕНИ ИЛИ ИДЕНТИФИКУВАНИ ИНЦИДЕНТИ НА МРЕЖНИТЕ И ИНФОРМАТИЧКИТЕ СИСТЕМИ

Член 1

Со овој правилник се пропишува начинот на пријава и постапување по пријавени или идентификувани инциденти на мрежните и информатичките системи во Владата на Република Северна Македонија и другите органи на државната управа, општините, општините во градот Скопје и градот Скопје.

Член 2

(1) Од страна на суштинските и важните субјекти под надлежност на MKD-GOV-CSIRT се известува надлежниот Тим за одговор на компјутерски безбедносни инциденти за било каков значаен сајбер-безбедносен инцидент и/или значајна закана за сајбер безбедноста што влијае на обезбедувањето на нивните услуги.

(2) Известувањето од ставот 1 на овој член, се врши без непотребно одлагање до три часа од моментот кога ќе се дознае за настанот и ги содржи сите информации потребни за да се утврди какво било прекугранично влијание на инцидентот, што е клучно за меѓународната координација.

(3) Доколку известувањето од ставот (1) на овој член, првично се достави до Министерството за дигитална трансформација, истото се препраќа до MKD-GOV-CSIRT без непотребно одлагање до два часа од приемот.

Член 3

(1) Од страна на суштинските и важни субјекти, доколку е можно се информираат нивните корисници на услуги кои потенцијално се погодени од сериозната закана за сајбер безбедност.

(2) Известувањето од ставот 1 на овој член, се прави веднаш, а најдоцна следниот работен ден од дознавањето за заканата и содржи информации за сите мерки или правни лекови што корисниците можат да ги преземат како одговор на заканата.

Член 4

(1) Од страна на суштинските и важни субјекти се обезбедува рано предупредување до GOV-CSIRT до 24 часа, откако ќе станат свесни за значајниот сајбер безбедносен инцидент, кое треба да укаже дали постои сомнеж дека инцидентот бил предизвикан од незаконски или злонамерни дејства, или дали може да има влијание во странство.

(2) По приемот на известувањето од ставот (1) на овој член, MKD-GOV-CSIRT започнува со проценки и се подготвува за потенцијални пошироки импликации.

(3) Од страна на суштинските и важни субјекти 72 часа од дознавањето за значајниот сајбер безбедносен инцидент се доставува подетален извештај за инцидент до MKD-GOV-CSIRT, со кој се ажурираат информациите за раното предупредување и вклучуваат

почетна проценка на сериозноста и влијанието на инцидентот, како и сите достапни индикатори за компромитирање, кое им овозможува на други субјекти и на MKD-GOV-CSIRT проактивно да откриваат, блокираат и да се бранат од слични методологии на напади, трансформирајќи ги индивидуалните инциденти во можности за колективно учење.

(4) MKD-GOV-CSIRT може да побара повремени извештаи за релевантни ажурирања на статусот додека напредува одговорот на инцидентот, што му овозможува да одржува свесност за ситуацијата и да обезбедува континуирани насоки.

(5) Од страна на суштинските и важните субјекти се доставува сеопфатен конечен извештај до MKD-GOV-CSIRT еден месец од поднесувањето на првичниот извештај за инцидентот кој содржи детално опишување на инцидентот (сериозност и влијание), веројатниот тип на закана или главна причина, применети и тековни мерки за ублажување, и прекугранично влијание, доколку такво постои, кој е клучен за научени лекции и долгорочни подобрувања на безбедноста.

(6) Ако значајниот сајбер-безбедносни инцидент трае во моментот кога треба да се достави конечниот извештај од ставот (5) на овој член, субјектот доставува извештај за напредок на инцидентот во тој момент и поднесува конечен извештај во рок од еден месец по целосно решавање на инцидентот.

Член 5

Офицерите за сајбер безбедност ги пријавуваат значајните сајбер безбедносни инциденти до MKD-GOV-CSIRT и ги даваат потребните известувања согласно членот 8 од овој правилник.

Канали за пријавување и технички барања

Член 6

(1) Ефикасното известување за инциденти се потпира на јасно дефинирани, безбедни и достапни канали.

(2) Суштинските и важни субјекти регистрираат и пријавуваат сајбер-безбедносни инциденти преку портал, обезбедувајќи стандардизиран и конзистентен механизам за пријавување.

(3) Сите податоци наменети за Националниот регистар на сајбер инциденти ќе се генерираат преку порталот од ставот (2) на овој член.

(4) MKD-GOV-CSIRT одржува повеќе различни комуникациски канали за пријавување на сајбер безбедносни инциденти, надвор од порталот од ставот (2) на овој член, кои се континуирано достапни.

(5) Каналите за комуникација од ставот (1) на овој член, се дизајнирани на начин кој гарантира редундантност, осигурувајќи дека прекинот на еден канал не води до целосен комуникациски прекин.

(6) Каналите за комуникација од ставот (1) на овој член треба јасно да бидат наведени на официјалната веб-страница на Министерството за дигитална трансформација и проследени до сите заинтересирани субјекти за да се обезбеди лесен пристап и јасност во начините за пријавување.

(7) MKD-GOV-CSIRT ја промовира употребата на безбедни дигитални алатки за размена на информации, поттикнувајќи безбедна комуникациска средина за сите засегнати страни, која вклучува примена на вообичаени или стандардизирани практики, шеми за класификација и таксономии воспоставени од Националниот тим за одговор на инциденти со компјутерска безбедност (MKD-CIRT) за процедури за ракување со инциденти, управување со кризи и координирано откривање на ранливости.

(8) Деталните технички и процедурални барања за известување и комуникациските канали обезбедуваат не само прием на информации, нивен интегритет, доверливост и употребливост за брза анализа и одговор.

Член 7

По добивањето извештај за значаен сајбер безбедносен инцидент, MKD-GOV-CSIRT презема активности за да обезбеди брз и ефикасен одговор кои вклучуваат:

- потврда и почетна повратна информација (24 часа од раното предупредување);
- по барање од суштински или важен субјект, MKD-GOV-CSIRT дава насоки или оперативни совети за спроведување на можни мерки за ублажување на инцидентот;
- доколку побара засегнатиот субјект, MKD-GOV-CSIRT обезбедува дополнителна техничка поддршка;
- од страна на MKD-GOV-CSIRT се собираат и анализираат форензички податоци поврзани со инцидентот за да го разбере неговиот обем, влијание и основна причина;
- од страна на MKD-GOV-CSIRT се врши динамична анализа на ризици и инциденти за да ги подобри тековните напори за одговор и да обезбеди свесност за ситуацијата;
- ако е можно, MKD-GOV-CSIRT доставува рани предупредувања, аларми, известувања и информации за сајбер закани, ранливости и инциденти до други суштински и важни субјекти, надлежни органи и засегнати страни;
- ако инцидентот се однесува на повеќе земји, од страна на MKD-GOV-CSIRT веднаш се известува Министерството за дигитална трансформација, кое потоа ги известува засегнатите земји без одлагање (најдоцна до два часа од дознавањето) и обезбедува релевантни информации, додека ги штити безбедноста, комерцијалните интереси на субјектот и доверливоста. Детален извештај за прекугранични инциденти се доставува до Министерството за дигитална трансформација пет дена по надминувањето на инцидентот, кој потоа го проследува до погодените земји во рок од два дена.
- ако постои сомнеж дека е извршено кривично дело, од страна на MKD-GOV-CSIRT се даваат насоки за пријавување на инцидентот до надлежните органи.
- ако е неопходна јавна свест за спречување или решавање на тековен значаен инцидент, или ако откривањето е во јавен интерес, Министерството за дигитална трансформација (по консултација со засегнатиот субјект) може да ја информира јавноста или да побара од субјектот да го стори тоа.
- од страна на MKD-GOV-CSIRT се води евиденција за пријавени инциденти поврзани со мрежата и информациските системи на институциите од јавниот сектор под негова надлежност.
- од страна на MKD-GOV-CSIRT веднаш се известува Националниот тим за одговор на компјутерски безбедносни инциденти (MKD-CIRT) за настаните инциденти, најдоцна пет дена од настанот, со цел ажурирање на Националниот регистар на сајбер инциденти.

Член 8

Од страна на MKD-GOV-CSIRT се преземаат проактивни мерки за откривање на закани и ранливости во рамките кои опфаќаат:

- следење и анализа на сајбер закани, ранливости и инциденти што ги засегаат субјектите под негова надлежност;
- По барање, се обезбедува помош на суштински и важни субјекти во следење на нивната мрежа и информациски системи во реално време;
- MKD-GOV-CSIRT може да спроведе проактивно неинвазивно скенирање на јавно достапни мрежни и информациски системи на суштински и важни субјекти под нејзина надлежност. Ова скенирање се изведува со цел да се идентификуваат ранливи или лошо

конфигурирани мрежни и информациски системи. Таквото скенирање е дизајнирано да нема негативно влијание врз функционирањето на услугите што ги обезбедува операторот. Од страна на MKD-GOV-CSIRT се информираат субјектите чија мрежа и информациски системи биле скенирани за резултатите од ова проактивно скенирање.

- По барање од суштински и важни субјекти или надлежни органи, од страна на MKD-GOV-CSIRT може да се обезбеди проактивно скенирање на нивната мрежа и информациски системи за идентификување ранливости со потенцијал за значително влијание.

- од страна на MKD-GOV-CSIRT може да се приоретизираат одредени задачи, вклучувајќи проактивни напори за идентификација, врз основа на спроведена анализа на ризик.

Член 9

Овој правилник влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 10-1443/1
23 јуни 2026 година
Скопје

Министер за дигитална
трансформација,
Стефан Андоновски с.р.