MKD-CIRT · АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

Пријава на компјутерски безбедносен инцидент

Образец за офлајн пополнување · член 33 од Законот за безбедност на мрежни и информациски системи

Значаен инцидент се пријавува најдоцна 3 часа од дознавањето.
Пополнете го она што е познато, а останатото дополнете го со следните известувања (24 ч, 72 ч, завршен извештај). Пополнетиот образец испратете го на soc@mkd-cirt.mk, шифриран со PGP клучот на MKD-CIRT (0x333C00DB). Во итни случаи јавете се на +389 2 3091 232. Полињата означени со * се задолжителни.

ПРИЈАВА

Ниво на заштита на доставената информација *

- ○ Строго доверливо
- ○ Доверливо
- ○ Јавно

Фаза на известување *

- ◉ Првично известување (до 3 часа)
- ○ Известување за инцидентот (до 72 часа)
- ○ Завршен извештај
- ○ Рано предупредување (до 24 часа)
- ○ Привремен извештај (на барање на MKD-CIRT)
- ○ Доброволна пријава

Број на предмет кај MKD-CIRT

Само при ажурирање: од потврдата за прием на првичното известување.

Ознака за споделување (TLP) *

- ○ TLP:RED
- ○ TLP:AMBER+STRICT
- ○ TLP:AMBER
- ○ TLP:GREEN
- ○ TLP:CLEAR

RED – само именувани примачи; AMBER+STRICT – само вашата организација; AMBER – организацијата и нејзините клиенти; GREEN – заедницата; CLEAR – без ограничување.

ПОДАТОЦИ ЗА СУБЈЕКТОТ

Назив на субјектот *

Сектор

Категорија на субјектот *

- ○ Суштински субјект
- ○ Важен субјект
- ○ Друго / доброволна пријава
- ○ Не знам

ЛИЦЕ ЗА КОНТАКТ

Одговорно лице (име и презиме) *

Е-пошта *

Телефон *

ИНЦИДЕНТ

Тип на инцидент *

Изберете ја категоријата што најдобро го опишува инцидентот.

- ○ **Abusive Content**
  Спам, злонамерна или незаконита содржина, злоупотреба на комуникациски канали и други форми на недозволена содржина.
- ○ **Malicious Code**
  Злонамерен софтвер, ransomware, wiper, botnet, backdoor, тројанци, црви, cryptominer и слични појави.
- ○ **Information Gathering**
  Скенирање, прибирање информации, sniffing, social engineering, phishing и други подготвителни активности.
- ○ **Intrusion Attempts**
  Обиди за неовластен пристап, brute force, exploit attempts и искористување ранливости без потврден успешен пробив.
- ○ **Intrusions**
  Успешен неовластен пристап, компромис на сметки, апликации, системи или мрежи.
- ○ **Availability**
  DoS/DDoS, sabotage, outage, прекин или значајна деградација на услуга.
- ○ **Information Content Security**
  Неовластен пристап, измена, губење, протекување или компромис на податоци.
- ○ **Fraud**
  Измама, кражба на идентитет, злоупотреба на ресурси или акредитиви.
- ○ **Vulnerable**
  Откриени ранливи, погрешно конфигурирани или изложени системи без потврдена експлоатација.
- ○ **Other / Test**
  Инциденти кои не се вклопуваат во претходните категории, односно тест-записи кои јасно се означуваат како тест.

Датум и час на дознавање *

дд.мм.гггг чч:мм · од овој момент течат роковите

Датум и час на настанување

дд.мм.гггг чч:мм · ако е познато

Наслов *

Опис на инцидентот *

Што се случило, како е откриено, кои се првите сознанија.

Засегнати услуги и системи

Услуги, системи, локации, приближен број на засегнати корисници.

Проценето влијание и сериозност

Прекин или нарушување на услугите, финансиска загуба, штета за корисници или други лица.

Сомнеж за злонамерно или незаконито дејство

○ Да ○ Не ○ Непознато

Можно прекугранично влијание

○ Да ○ Не ○ Непознато

ТЕХНИЧКИ ДЕТАЛИ И МЕРКИ

Показатели на компромитираност (IOC)

IP адреси, домени, URL, хеш вредности, е-адреси на испраќачи.

Преземени мерки

Изолација, блокирање, промена на лозинки, сочувани логови.

Потребна помош од MKD-CIRT

Анализа, координација, насоки за ублажување.

ИСПРАЌАЊЕ

Место и датум на пополнување

Пополнил (име, функција)

Пополнетиот образец испратете го на soc@mkd-cirt.mk. Ако содржи чувствителни податоци, шифрирајте го со PGP клучот на MKD-CIRT (Key ID 0x333C00DB, fingerprint 0FB9 3DA3 E008 FA8B FC6A 9C71 0741 17A1 333C 00DB). Прилозите (логови, примероци) испратете ги шифрирани или како архива со лозинка доставена по друг канал. Онлајн пријава: mkd-cirt.mk/onlajn-prijava.