**УТВЪРДИЛ:**

ВЛАДИМИР ГЕОРГИЕВ

Кмет на Община Самоков

# ВЪТРЕШНИ ПРАВИЛА ЗА УПРАВЛЕНИЕ НА ИНЦИДЕНТИ В ОБЩИНСКА АДМИНИСТРАЦИЯ САМОКОВ

**гр. Самоков**

**2020 година**

# I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите правила са разработени на основание чл.30, ал.1-4 и чл.31, ал.1-4 от „НАРЕДБА за минималните изисквания за мрежова и информационна сигурност“.
2. Целта на този документ е да се определи: редът за идентификация на събитие, редът за категоризиране и приоритизиране на инциденти, ролите и отговорностите на служителите и трети страни при управлението на инцидентите.
3. Вътрешните правила регламентират всички дейности при обработката на сигнали и реакция при инциденти.
4. Настоящият документ се преглежда за адекватност редовно от Съвет за мрежова и информационна сигурност, като при необходимост се актуализира.

# II. ТЕРМИНИИ И ДЕФИНИЦИИ

4. **Събитие** - идентифицирана случка по отношение на състоянието на система, услуга или мрежа, показваща възможен пробив в политиката за сигурност на информацията или отказ на защитите, или предварително неизвестна ситуация, която може да бъде свързана със сигурността.
5. **Инцидент** - отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията, които с голяма вероятност могат да предизвикат компрометиране на бизнес дейностите, и които заплашват сигурността на информацията.
6. **Значим инцидент** - отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията,

които могат да предизвикат катастрофални последици за бизнес дейностите и сигурността на информациятаРезервирането и/ или архивирането на информацията се извършва от служител в отдел ИКТ.

# III. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

5. Отговорен за управлението на инциденти е Съвета за мрежова и информационна сигурност.
6. Служителите и заинтересованите страни подават сигнали за настъпили или потенциални събития, оказващи негативно влияние върху мрежовата и информационната сигурност към Съвета за мрежова и информационна сигурност (СМИС) на телефон: 0888355055 или електронна поща: admin.samokov@samokov.bg.
7. Постъпилият сигнал се регистрира в „Искане за инцидент“ (Приложение 1 на настоящите правила) от член на Съвета за мрежова и информационна сигурност. последващото уведомяване за това на подателя.
8. Регистрираният инцидент се предава на Главен експерт КС за проверка на достоверността на сигнала. Установените данни със свръзка с инцидента се документират допълнително в „Искането за инцидент“, като се класифицира и се определя приоритета.
9. Установеният инцидент се анализира и се определят мерки, които да се предприемат за прекратяване на негативното действие.
10. СМИС запознава Кмета на Общинската администрация за всички инциденти с висок и среден приоритет.
11. СМИС запознава заинтересованите страни и подателите за всички инциденти с нисък и среден приоритет и предприетите действия по прекратяване на негативното действие.
12. Кметът на Общината уведомява всички заинтересовани страни при установен инцидент с висок приоритет и ги информира за предприетите действия по прекратяване на негативното действие.

13. Ефективността на предприетите мерки се наблюдава и оценява от Главен експерт КС, който определя инцидента за приключен ако няма нови събития.
14. Всички долазателства свързани с инцидента (логове, snapshots, записи и др.) се събират от служителите работили по инцидента и се предават на СМИС за съхранение, които да послужат за извършването на процесуални действия срещу лице или организация ако инцидента предполага подобни искания.
15. Достъп до записите и доказателствата свързани с инцидентите имат Кмета, Председателя и членовете на СМИС.
16. СМИС разработва, проверява и поддържа в актуално състояние планове за справяне с инцидентите (Приложение 3), които биха имали най-сериозно въздействие върху мрежовата и информационната сигурност.

# IV. УВЕДОМЯВАНЕ ЗА ИНЦИДЕНТИ НА СЕКТОРНИЯ ЕКИП

17. При инцидент с мрежовата и информационната сигурност Съвета за мрежова и информационна сигурност, уведомява секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност.
18. Първоначално уведомяване се прави до 2 часа след констатирането на инцидента. Уведомленията се подават по образец, който е приложение към настоящите правила и съдържа информация, която дава възможност на секторния екип да определи евентуалното трансгранично въздействие на инцидента.
19. В срок до 5 работни дни Съвета за мрежова и информационна сигурност предоставя на секторния екип пълната информация за инцидента.
20. В случай че информацията за инцидентите се изпраща по електронна

поща, тя трябва да е подходящо защитена от неоторизиран достъп и да е класифицирана съгласно Вътрешните правила за класификация на информацията.

Приложение 1

**УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ**

**към секторния ЕРИКС**

| **Необходима информация** | **Детайли** | **Данни** |
|---|---|---|
| **(до 2 часа)** | | |
| Лице, подаващо уведомлението | Име, фамилия | |
| Вашият телефонен номер | (GSM) | |
| Вашата електронна поща | | |
| Организация | Наименование на организацията, засегната от инцидента | |
| Лице за контакт (за целите на разрешаването на инцидента) | Име, телефонен номер и електронна поща на компетентно лице от предприятието, което при необходимост може да подаде допълнителна информация | |
| Дата и час | Вписват се датата и часът на възникване на инцидента, ако не е възможно - датата и часът на откриването му | |
| Тип на инцидента | | 0 Virus 0 Trojan 0 Botnet 0 Dos/DDos 0 Malware<br>0 Port Scan 0 Spam 0 Phishing 0 Pharming<br>0 Probe 0 Crack 0 Copyright 0 Ransomware<br>0 Defacement 0 Exploiting known |

**УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ**

**към секторния ЕРИКС**

| **Необходима информация** | **Детайли** | **Данни** |
|---|---|---|
| | | Vulnerabilities<br>0 Application Compromise 0 Login Attempts<br>0 SQL injections<br>0 Unknown<br>0 Other |
| Кратко описание на инцидента | Вписва се кратко описание на инцидента, като се включва всяка практическа/техническа информация (тази информация се предоставя, в случай че е налична) | |
| Трансгранично въздействие | • Вписва се информация за евентуално трансгранично въздействие и се посочват държавите<br>• Вписва се информация за услугите, които са засегнати | |
| Въздействие върху други съществени услуги | Вписва се информация на кои други съществени услуги евентуално ще окаже въздействие | |
| Засегната система (попълва се, ако е налична информацията) | IP Address:<br>DNS:<br>Operating System: | |
| Източник на атаката (попълва се, ако е налична информацията) | IP Address:<br>DNS: | |
| Предприети | Описват се първоначалните | |

**УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ**

**към секторния ЕРИКС**

| **Необходима информация** | **Детайли** | **Данни** |
|---|---|---|
| действия | действия, предприети до момента - до 2 часа от засичането на инцидента | |
| Публично оповестяване | Съгласно комуникационна стратегия на администрацията | |
| **до 5 работни дни** | | |
| Механизъм на атаката | Описва се механизмът на атаката | |
| Предприети действия | Описват се подробно действията, предприети за разрешаване на инцидента | |
| Необходимост от коригиращи действия | Има ли необходимост от промяна в настройките на защитните стени, WAF или др.<br>Промяна на политиката за сигурност, ако се налага<br>Обучение на персонала | |
| Анализ на артефаки | Описват се резултатите от анализа на артефактите, ако има установени такива, и инструментите, използвани за това.<br>Изпраща се копие от артефактите | |
| Публично оповестяване | Съгласно комуникационна стратегия на администрацията | |

***Забележка.*** Попълва се допълнителна информация в случай на необходимост.

Приложение № 2

## КЛАСИФИКАЦИЯ НА ИНЦИДЕНТИТЕ И ПРИОРИТЕТ

| Клас | Тип на инцидента | Приоритет | Описание/пример |
|---|---|---|---|
| Abusive Content | Spam | Нисък | "Нежелана електронна поща". Използването на среда за електронни комуникации (интернет) за масово изпращане на нежелани съобщения. Spam съобщенията се изпращат като част от по-голяма колекция от съобщения, всички с идентично съдържание. |
| | Harassment | Нисък | Компромати или дискриминация спрямо някой (пр. cyberstalking). |
| | Child/sexual/violence/... | Висок | Детската порнография, прослава на насилието, ... |
| Malicious Code | Virus | Среден | Софтуер, който преднамерено се инсталира в системите с вредни цели. Необходимо е действие на потребителя, за да се активира кодът. |
| | Worm | Среден | |
| | Trojan | Среден | |
| | Spyware | Среден | |
| | Dialer | Среден | |
| Information Gathering | Scanning | Среден | Атаки, които изпращат заявки към дадена система с цел да открият слаби места. Това включва също и някои видове тестове с цел да се събере информация за хостове, услуги и сметки. Примери: fingerd, DNS заявки, ICMP, SMTP (EXPN, RCPT, ...). |
| | Sniffing | Нисък | Наблюдение и записване на мрежовия трафик (wiretapping) |
| | Social engineering | Нисък | Събиране на информация от индивиди без използване на технически средства (например, лъжи, трикове, подкупи или заплахи). |
| Intrusion Attempts | Exploiting known vulnerabilities | Среден | Опит да се компрометира система или да се наруши целостта на услуга, като се използва уязвимост със стандартизиран идентификатор, като CVE име (например, buffer overflow, backdoors, cross site scripting, и т.н.). |
| | Login attempts | Среден | Множество опити за логване в система (пр. guessing/cracking of passwords, brute force). |
| | New attack signature | Нисък | Опит за атака, използваща нови техники. |

| | | | |
|---|---|---|---|
| Intrusions | Privileged account compromise | Среден | Успешен пробив в система или приложение (услуга). Това може да е причинено дистанционно чрез използване на известна или нова уязвимост, както и локално от неоторизирано лице. |
| | Unprivileged account compromise | Среден | |
| | Application compromise | Среден | |
| Availability | DoS | Висок | В този вид атака системата се бомбардира с толкова много пакети, че процесите се забавят или системата блокира. Примери за отдалечен DoS са SYN- и PING-flooding, бомбардиране на електронна поща и др. (DDoS: TFN, Trinity и др.) Въпреки това наличността на услугите може да бъде засегната и от действия на локално ниво (унищожаване, прекъсване на електро-захранването и др.) |
| | DDoS | Висок | |
| Information Security | Sabotage | Висок | |
| | Unauthorized access to information | Среден | Освен локални злоупотреби с данни и системи, сигурността на информацията може да бъде застрашена и от успешно компрометиране на акаунти и приложения. В допълнение на това са възможни и атаки, които прихващат и достъпват информация по време на нейното предаване (подслушване, подправяне или прихващане). |
| | Unauthorized modification of information | Среден | Опит за атака, използващ нови техники. |

| | | | |
|---|---|---|---|
| Fraud | Unauthorized use of resources | Среден | Използване на ресурси за непозволени цели, включително парично облагодетелстване (например, използването на електронна поща за участие в незаконно разпращане на писма с цел облагодетелстване или участие в пирамидални схеми за източване на данни и средства).<br>Продажба и инсталиране на нелицензирани копия на търговски софтуер или други защитени с права търговски материали (Warez).<br>Видове атаки, в които едно лице незаконно приема самоличността на друго, за да се възползва от него. |
| | Copyright | Нисък | |
| Other | Masquerade | Висок | |
| | Phishing | Висок | Атака, при която е създадено копие на легитимна WEB страница, през която жертвите са подмамвани да въвеждат лични данни или друга конфиденциална информация. Въведените данни се използват по-нататък за незаконни дейности.<br>За всички инциденти, които не попадат в по-горната класификационна схема. |
| | | | |

Приложение № 3

## ПЛАН ЗА СПРАВЯНЕ С ИНЦИДЕНТИТЕ

| | |
|---|---|
| Отговорник при настъпване на инцидент | |
| Ред за информиране | |
| Мерки, които следва да се предприемат и отговорното за това лице | |
| Ред за консултиране | |
| Ред за следене на параметрите по време на инцидента | |
| Служител, който ще събира и съхранява необходимата информация, и др | |