Типовые инциденты ИБ и процедуры реагирования на них

К типовым инцидентам ИБ относятся:

- нарушение установленного в организации режима доступа к информации или компонентам:
  - неправомерный доступ к информации
  - утечка конфиденциальной информации
  - удаление информации
- превышение допустимой нагрузки на вычислительные ресурсы (атака типа «отказ в обслуживании» (DDoS))
- отказ используемого программного обеспечения

Реагирование на инцидент ИБ включает в себя:

- технические мероприятия, обеспечивающие целостность значимых данных (путем отключения, упаковки (клонирования), а затем и должного хранения соответствующих носителей информации) и возможность исследования этих данных в будущем
- организационные мероприятия по уведомлении руководства и подразделений информационной безопасности организации, анализу инцидента и введению изменений корпоративных процессов, которые позволяют снизить ущерб от происшедшего инцидента и предотвратить в будущем

В случае возникновения инцидента ИБ необходимо:

1. Идентифицировать инцидент и убедиться, что он действительно имеет место быть.
2. Локализовать область инфраструктуры и ПО, задействованной в инциденте.
3. Ограничить доступ к объектам, задействованным в инциденте.
4. Оформить служебную записку на имя руководителя организации о факте возникновения инцидента.
5. Снять энергозависимую информацию с работающей системы.
6. Собрать информацию о протекающем в реальном времени инциденте.
7. В присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образов и другой информации для последующего анализа и сохранения.
8. Оформить протоколом все операции с носителями информации.

9. Провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения.
10. Передать носителей на исследование в службу ИБ.
11. После сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем.
12. При проведении исследования источников информации обеспечить неизменность доказательств. Работать только с копией.
13. По завершении исследования и анализа инцидента составить отчет и рекомендации по снижению рисков возникновения подобных инцидентов в будущем.

Вероятные инциденты в продукте Cloudmaster

Попытка подбора пароля пользователя

Определяется неоднократным событием CM-00011 с одного и того же IP-адреса (атрибут src в поле Extension).

Рекомендуемое реагирование - заблокировать в сервисе аутентификации (корпоративном каталоге УЗ) УЗ пользователя (атрибут suser в поле Extension), связаться с пользователем.

Попытка выхода за границы привилегий

Т.к. в панелях управления отображаются только допустимые операции для данной роли (с которой произошла аутентификация), то единственный способ выполнить неправомерную операцию - целенаправленно создать и попытаться выполнить API-запрос.

Попытка определяется событием CM-00080.

Рекомендуемое реагирование - заблокировать в сервисе аутентификации (корпоративном каталоге УЗ) УЗ пользователя (атрибут suser в поле Extension), связаться с пользователем.

Попытка подменить сервис аутентификации (корпоративный каталог УЗ)

(а) Попытка определяется событием CM-00070.

Рекомендуемое реагирование - проверить IP-адрес или FQDN сервиса аутентификации с фактически актуальными в корпорации. В случае несовпадения - заблокировать в сервисе аутентификации (корпоративном каталоге УЗ) УЗ пользователя (атрибут suser в поле Extension), связаться с пользователем, изменить в настройках Cloudmaster параметры интеграции с корпоративным каталогом УЗ на верные.

(б) Попытка определяется событием CM-00090 и атрибутом app=LDAPS в поле Extension.

Рекомендуемое реагирование - проверить IP-адрес и FQDN сервиса аутентификации (атрибуты dst и dhost в поле Extension) с фактически актуальными в корпорации. В случае несовпадения - изменить в настройках.