Общество с ограниченной ответственностью "АВС"
(ООО "АВС")

УТВЕРЖДАЮ
Председатель правления ООО "АВС"

_____ Иванов А. Г.

29.07.2024

План реагирования на инциденты ИБ

Общие положения

1**. Цель**: обеспечение быстрого и эффективного реагирования на инциденты ИБ, минимизация ущерба и восстановление нормальной работы информационных систем.
2. **Область применения**: вся информационная инфраструктура компании ООО «АВС».
3. **Ответственные лица**:

Начальник отдела информационной безопасности: несёт ответственность за обеспечение защиты информации в компании.

Руководитель группы реагирования: отвечает за координацию действий рабочей группы, принятие решений и взаимодействие с руководством компании.

Члены рабочей группы: специалисты по информационной безопасности, системные администраторы, технические специалисты и другие сотрудники, необходимые для реагирования на инцидент.

Порядок реагирования:

Обнаружение и анализ: обнаружение происходит с помощью правильно настроенных инструментов, например, «сработок» систем мониторинга (алертов) по настроенным правилам, иногда инциденты выявляют люди при ручном анализе событий. Сотрудник или система, обнаружившие инцидент, должны немедленно уведомить руководителя группы реагирования и людей которые необходимы для дальнейшей работы с инцидентами. Руководитель группы оценивает степень угрозы, масштаб инцидента и возможные последствия. Инцидент классифицируется и определяется его приоритетность. Ответственный сотрудник должен зафиксировать инцидент — занести информацию в журнал инцидентов. Рабочая группа проводит детальный анализ инцидента, уточняет затронутую область и пострадавшие объекты. Параллельно — на основании предварительной оценки ущерба и влияния — принимается решение об уведомлении вышестоящего руководства, регуляторов. В случае если инцидент влечёт утечку данных или нарушение функционирования публичного сервиса, может приниматься решение об уведомлении СМИ.

Локализация, ликвидация и восстановление: изоляция задетых инцидентом устройств на уровне сети и при необходимости временная остановка потенциально скомпрометированных бизнес-процессов. Выявление механизмов воздействия и степени воздействия. Анализируются логи, включая логи других систем для поиска следов атаки и аномалий. Снимаются дампы, происходит

нейтрализация и устранение инцидента, восстановление системы к первоначальному состоянию, при необходимости установка обновлений и фиксов безопасности.

Меры, принимаемые после инцидента: оформление сводки по инциденту (post mortem) с описанием причины возникновения инцидента, хронологию всех событий, принятые решения, ущерб и последствия инцидента, итоги расследования и итоги восстановления функционирования системы. Наиболее критичные данные по инцидентам заносятся в базу знаний и пополняют базу Threat Intelligence. При необходимости принимаются дополнительные организационные и технические меры.

Порядок реагирования на общие инциденты

1. Сотрудник или система, выявившие инцидент, уведомляют руководителя группы реагирования и людей которые необходимы для дальнейшей работы с инцидентами

2. Руководитель группы оценивает ситуацию и принимает решение о необходимости привлечения дополнительных ресурсов.

3. Рабочая группа выполняет следующие действия:

- изолирует затронутые системы;

- собирает информацию об инциденте;

- анализирует данные;

- определяет причину инцидента;

- разрабатывает план устранения последствий;

- устраняет последствия инцидента;

- восстанавливает нормальную работу систем;

- документирует все действия и результаты.

Реагирование на конкретные виды инцидентов

При выявлении вредоносного ПО на серверах компании:

- Немедленно отключить заражённые серверы от сети.

- Собрать информацию о заражённых серверах: IP-адреса, имена хостов, версии операционных систем и приложений.

- Проанализировать данные и определить тип вредоносного ПО.

- Определить источник заражения и способы распространения.

- Разработать план удаления вредоносного ПО и восстановления нормальной работы серверов.

- Удалить вредоносное ПО с серверов и восстановить их работоспособность.

- Провести анализ уязвимостей и принять меры по их устранению.

- Документировать все действия и результаты.

- Сообщить руководству компании о результатах расследования и принятых мерах.

При выявлении DdoS-атаки:

- Использовать средств фильтрации трафика, такие как межсетевые экраны (Firewall), системы обнаружения и предотвращения вторжений (IDS/IPS) и другие технологии, которые могут помочь отсеять нежелательный трафик и снизить нагрузку на серверы.

- При необходимости временно ограничить доступ к определённым ресурсам или сервисам компании, чтобы уменьшить воздействие атаки. Это может быть полезно в случае, если атака направлена на конкретный сервис или приложение.

- Задействовать специализированные решения для защиты от DDoS-атак, которые могут помочь предотвратить или минимизировать их воздействие. Такие системы могут включать в себя балансировку нагрузки, кеширование, защиту от атак на уровне приложений и другие функции.

- Обратиться к своему провайдеру услуг связи для получения дополнительной поддержки и информации о происходящем.

- Провести анализ результатов атаки, устранить выявленные недочёты, при необходимости добавить новые меры защиты и улучшенные алгоритмы обнаружения атак.

- Задокументировать все действия и результаты.

- Сообщить руководству компании о результатах расследования и принятых мерах.

При выявлении утечки персональных данных:

- Немедленно приостановить распространение утечки, отключив затронутые системы и ограничив доступ к ним.

- Оценить масштаб и характер утечки, включая количество затронутых записей, типы данных и потенциальные последствия для клиентов.

- Определить источник утечки, причины, способ, тип (случайная или намеренная, внутренняя или извне), организовать внутреннее расследование при необходимости задействовать службу безопасности.

- Собрать все необходимые доказательства и документацию, связанные с инцидентом.

- Сообщить руководству компании о результатах расследования и принятых мерах.

- Сообщить о происшествии в соответствующие органы (например, Роскомнадзор, ФСБ) в определенный требованиями срок.

Начальник отдела
информационной безопасности Петров Б. В.

29.07.2024