Подготовка 1

Установить контакты, выработать процедуры, собрать необходимую информацию и ознакомиться с доступными системами обнаружения сетевых вторжений для оптимизации временных затрат на момент инцидента.

Обнаружение Сетевых Вторжений

- Убедиться, что средства мониторинга и анализа сетевых вторжений находятся в рабочем и актуализованном состоянии.
- Установить рабочие контакты с внутренними командами сетевой и информационной безопасности.
- Формализовать процесс уведомлений об обнаружении вторжений; сообщите вовлеченным командам.

Сеть

- Убедиться в существовании подробного списка точек сетевого доступ. Поддерживать документ в актуализованном состоянии.
- Убедиться в наличии у вовлеченных команд подробных планов и конфигураций сети.
- Регулярно проводить поиск нежелательных точек сетевого доступа (xDSL, WiFi, Modem) и закрывать обнаруженные объекты.
- Убедиться в эксплуатационной пригодности существующих инструментов и процессов администрирования сетевого траффика.

Стандартный траффик

- Определить характеристики базового траффика и сетевых процессов;
- Выявить критические производственные процессы.

Обнаружение 2

Вовремя обнаружить инцидент, определить затрагиваемый периметр производственной инфраструктуры и предупредить компетент-ных лиц.

Источники обнаружения

- Уведомление пользователем / службой поддержки
- IDS alert
- Обнаружение сотрудниками сетевой поддержки
- Жалоба из внешнего источника

Запись подозрительной сетевой активности

Сохранить сетевые пакеты в виде файла (PCAP) и передать расследующей инцидент команде для анализа.

Для сбора и записи пакетов возможно использовать Wireshark, Windump, Tcpdump, а также хаб или зеркалирование портов на подверженной атаке LAN-сети.

Использование методов сетевой компьютерной криминалистики требует специальных навыков и знаний. Не стесняйтесь обратиться к специалистам из вашей команды реагирования за помощью или советами.

Анализ атаки

- Проанализировать поступившие оповещения IDS.
- Просмотреть статистику логов и сетевых устройств.
- Постараться определить цели вредоносного траффика и затронутые компоненты инфраструктуры.
- Определить технические характеристики траффика:
  - Исходные IP адреса
  - Используемые порты, TTL, Packet ID, …
  - Используемые протоколы
  - Атакуемое оборудование или сервисы
  - Используемые уязвимости и эксплойты
  - Удаленно-авторизованные учетные записи

Цель этапа - определить мишени и способы атаки, а также исходные IP атакующей стороны. Для этого возможно применение методов компьютерной криминалистики. В случае обнаружения скомпрометированной машины, воспользуйтесь соответствующей IRM.

Сдерживание 3

Минимизировать последствия инциден-та на IT-ресурсы.

В случае, если инцидент затрагивает стратегические ресурсы, предприятия, возможна мобилизация целевой Кризисной Группы.

В зависимости от уровня критичности затронутых ресурсов, возможно выполнение следующих действий:

- Отключить скомпрометированную часть сети от Интернета.
- Изолировать источник атаки. Отключить затронутую машину для дополнительного расследования.
- Найти меры по смягчению последствий инцидента на стратегический производственный траффик и согласовать их применение с руководством.
- Завершить нежелательные соединения и процессы на затронутых машинах.
- Создать правила firewall/IPS для блокировки атак.
- Информировать техническую команду по обнаружению новых совпадений с IDS правилами для калибровки.

При обнаружении серьезных инцидентов, применить следующие меры:

- Блокировать попытки организации утечек данных посредством Интернет фильтрации.
- Обязать серверы со стратегическими данными блокировать любые попытки соединений со стороны скомпрометиро-ванных машин.
- Строго ограничить доступ к конфиденциальным данным;
- Создать фиктивные документы с водяными знаками для последующего использования в качестве доказательства факта кражи.
- Оповестить сотрудников об инциденте; сообщить о введенных ограничениях.
- Настроить verbose метод авторизации для атакуемых инфраструктур: хранить логи по авторизации на удаленном защищенном сервере.

Устранение 4

Принять меры для пресечения вредоносной активности

Блокировка источника

- Используя ранее выполненные результаты аналитических действий по обнаружению и локализации угрозы, идентифицировать все каналы связи, используемые атакующей стороной и заблокировать их по периметру вашей сети.
- Если источником атаки является инсайдер, привлечь к решению вопроса руководство, отдел кадров и юридический отдел.
- Если источником атаки является сторонний объект, рассмотреть возможность привлечения правоохранительных органов.

Ликвидация последствий

- Формализовать процесс ликвидации последствий инцидента. В случае необходимости, утвердить процесс экспертной структурой, например CERT/CSIRT/IRT командой, ответственной за зону инцидента.
- Также могут быть полезными процессы ликвидации последствий несанкционированного доступа, изложенные в соответствующей IRM.

Тестирование и исполнение

- Протестировать процессы ликвидации последствий инцидента. Убедиться, что он работают корректно и не ставят под угрозу никакие сервисы и процессы.
- Применить процессы ликвидации последствий инцидента после получения одобрения результатов тестов от производственного и IT департаментов.

Восстановление 5

Восстановить систему до нормального операционного состояния.

- Убедиться в нормализации сетевого траффика.
- Разрешить сетевой траффик, использованный злоумышленниками для проникновения.
- Восстановись соединения подсетей.
- Восстановить соединение локальной сети.
- Восстановить доступ в Интернет.

Проделать в пошаговом режиме, обеспечив необходимое техническое сопровождение.

После инцидента 6

Задокументировать детали инцидента_и собранные данные. извлечь уроки, оптимизировать процессы защиты.

Отчет
Написать отчет об инциденте и сделать его доступным вовлеченным лицам. В рамках отчета необходимо раскрыть следующие темы:

- Причины инцидента
- Действия и сроки
- Верные действия
- Неверные действия
- Стоимость инцидента

Капитализация опыта
Формализовать и задокументировать опыт, накопленный в результате управления инцидентом с целью увеличения эффективности будущих действий.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #5

Вредоносная сетевая активность

Анализ сетевой активности

Автор IRM: CERT SG
Версия IRM: 1.4 (RU)

Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.

Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

IRM предоставляет детальную информацию по каждой из фаз.