

Подготовка

1

■ Назначить ответственных лиц из каждого вовлеченного департамента для участия в Кризисной Группе (КГ). Внести подробные координаты членов кризисной группы в контактный список и распространить между участниками.

■ Убедиться в дееспособном, функциональном и актуализованном состоянии специализированного оборудования, как то антивирусы, IDS, анализаторы логов и т.п.

■ Убедиться в наличии актуализованной версии картографии сети и инвентаря аппаратного оборудования.

■ Выполнять регулярный мониторинг безопасности и своевременно информировать ответственных лиц о направлениях угрозы.

■ Убедиться в существовании формализованных и регулярно тестируемых процессов непрерывности производства в отношении критических объектов предприятия.

Обнаружение

2

Обнаружение заражения

Собрать, проанализировать и упорядочить информацию, поступающую из различных источников:

- Логи антивирусов
- Intrusion Detection Systems
- Подозрительные попытки подключений к серверам
- Аномально большое количество заблокированных учетных записей
- Подозрительный сетевой трафик
- Подозрительные попытки подключения к файерволам
- Увеличение количества звонков в центр поддержки
- Нехарактерная нагрузка или зависания
- Аномальное увеличение объемов исходящего почтового трафика

При обнаружении одного или нескольких из вышеперечисленных симптомов, лица, определенные на первой стадии (см. "Подготовка") сконтактируются и, в случае необходимости, создадут Кризисную Группу.

Идентификация инфекции

Проанализировать симптомы для идентификации вредоноса, выявления векторов заражения и определения способов противодействия.

Полезная информация может быть найдена в:

- Бюллетенях CERT/CSIRT
- Сторонних службах поддержки (Microsoft, антивирусные вендоры, и т.д.)
- Тематических ресурсах (Secunia, и т.д.)

Оповестить начальника отдела информационной безопасности. Оповестить CERT/CSIRT/IRT.

Определить периметр распространения вредоноса и уровень его воздействия на производственные процессы.

Сдерживание

3

Кризисная Группа должна выполнить следующие действия:

- Изолировать инфицированный сегмент сети от Интернета и других сетей.
- В случае невозможности изоляции критического производственного трафика, разрешить его, предварительно убедившись в невозможности распространения инфекции через данный вектор или найти обходные пути для его обеспечения.
- Нейтрализовать векторы распространения заражения. Вектором распространения может быть что угодно - от сетевого трафика до уязвимостей в ПО. Меры безопасности могут включать в себя установки патчей ПО, блокировку сетевого трафика, отключение отдельных устройств, и т.д.

Возможно использование:

- Patch deployment tools (WSUS)
- Windows GPO
- Внедрение правил файерволов
- Специальные операционные процедуры

Повторить вышеуказанные действия для каждой подсети в зоне действия вредоноса до полного предотвращения распространения заражения.

Рекомендуется осуществлять параллельный мониторинг всех действий с помощью спецсредств (антивирусная консоль, серверные логи, звонки в центр поддержки).

Необходимо держать весь процесс распространения вредоноса под четким контролем.

Мобильные устройства

Убедитесь в невозможности использования переносных компьютеров и жестких дисков, планшетов и смартфонов для распространения компьютерного червя. Блокируйте соответствующие соединения и оповестите конечных пользователей.

Устранение

4

Средства

Возможно использование следующих средств:

- Исправления ПО (Microsoft, Oracle, etc.)
- Актуализация антивирусных баз
- Сторонняя поддержка
- Инфобез ресурсы

Определить процесс по устранению вредоноса. Процесс должен получить одобрение компетентной внешней структуры, например вашей команды реагирования на инциденты ИБ.

Тестирование

Перед применением, необходимо протестировать процесс по устранению вредоноса для того, чтобы убедиться, что процесс работает корректно, не затрагивая работу информационных систем.

Применение

Применить средства устранения вредоноса. Возможно использование следующих средств:

- Patch deployment tools (WSUS)
- Windows GPO
- Актуализация баз антивирусов
- Ручное удаление вредоноса

Внимание: некоторые черви могут блокировать процессы развертывания методов устранения вредоносов. В этом случае необходимо применение альтернативных методов (ручное удаление).

Процесс устранения угрозы должен находиться под контролем Кризисной Группы.

Восстановление

5

Убедившись в корректном применении предыдущих мер, получить одобрение руководства для следующих шагов.

- Открыть внутренний трафик для ранее инфицированных сегментов сетей.
- Восстановить соединения подсетей
- Подключить переносные устройства
- Восстановить соединения локальной сети
- Восстановить доступ в Интернет

Проделать вышеперечисленное в пошаговом режиме, обеспечив технический контроль со стороны Кризисной Группы.

После инцидента

6

Отчет

Написать отчет об инциденте заражения; сделать отчет доступным членам Кризисной Группы. В рамках отчета необходимо раскрыть следующие темы:

- Причины инфекции
- 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.

Incident Response Methodology

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

IRM #1

Заражение вредоносным кодом

Руководящие принципы реагирования на инциденты заражения вредоносным кодом (Червь)

Автор IRM: CERT SG
Версия IRM: 1.3 (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:** подготовиться 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.