Подготовка 1

Установить контакты, выработать процедуры, собрать необходимую информацию для оптимизации действий на момент инцидента.

- Подготовить схему ПО компонентов на веб сервере.
- Создать резервную копию сайта, готовую к мгновенной публикации.
- Формализовать процедуру перенаправления посетителей на резервный веб-ресурс.
- Развернуть инструменты мониторинга для оперативного обнаружения аномалий на критических веб-ресурсах.
- Экспортировать логи веб сервера на безопасный сторонний сервер; синхронизовать время на обоих серверах.
- Создать список стороннего контента (статического и динамического), используемого веб-ресурсом, включая рекламный контент.
- Создать справочник контактов хостинг провайдера.
- Убедиться, что ваш хостинг провайдер включил журналирование всех событий.
- Создать и поддерживать в актуализованном виде подробную картографию сетевой инфраструктуры.

Обнаружение 2

Зафиксировать инцидент, определить затрагиваемый периметр, вовлечь компетентных лиц.

Источники обнаружения:

- Мониторинг веб-ресурсов: Изменение контента веб-ресурса - *“You’ve been pwn3d by xxx”*, так и незаметным - “iframe” инжект, белый текст на белом фоне, и т.п.
- Пользователи: уведомления, полученные от пользователей, столкнувшихся с проблемами при посещении вашего сайта.
- Инструменты безопасности: оповещения, полученные посредством надстроек безопасности, таких как, например, Google SafeBrowsing.

Убедиться в факте инцидента и определить его источник:

- Проверить статический веб контент, в особенности даты изменения и хэш файлов.
- Проверить файлы, полученные от сторонних контент провайдеров, в т.ч. рекламного характера.
- Проверить присутствующие гиперссылки, в т.ч. после src, meta, css, script, и т.п.
- Проверить лог файлы.
- Просканировать базы данных на предмет наличия вредоносного контента.

Внимание: Для верного понимания проблемы необходимо как можно тщательнее изучить исходный код веб ресурса. Удостоверьтесь, что проблема находится на вашем сервере, а не сервере стороннего провайдера, например хостящего баннеры третьей стороны.

Сдерживание 3

Минимизировать последствия инцидента.

- **Осуществить резервное копирование контента веб-сервера для последующей криминалистической экспертизы или анализа инцидента.** В идеале, сделать побитовую копию жесткого диска веб-сервера. Это позволит восстановить удаленные файлы.
- **Проверить карту сетевой архитектуры. Локализовать использованную злоумышленником уязвимость:**
  - проверить систему сервера хостинга
  - проверить запущенные сервисы
  - проверить подключения к потенциально скомпрометированным внешним ресурсам

Если источником атаки является внешний ресурс или сеть, отключить соединение физическим путем и начать расследование.

Постараться найти улики для каждого действия атакующей стороны:

- **Идентифицировать использованные способы проникновения в систему и устранить уязвимости:**

- Веб компоненты уязвимости, позволяющие доступ на запись: устранить уязвимость, применив патч производителя ПО.
- Открытая общая папка: закрыть доступ.
- SQL уязвимость, позволяющая iSQL: исправить код.
- Сторонние компоненты: приостановить использование стороннего контента.
- Измененные права администрирования: ограничить права.

- **При необходимости, развернуть временный сайт на отдельном веб-сервере**. Временный сайт должен содержать оригинальный контент (до дифейса) или специальное оповещение типа “Temporary unavailable”. Лучше всего отобразить временный статический контент в HTML. Это позволит избежать дальнейшего использования возможных уязвимостей в оригинальном PHP/ASP/CGI/PL коде атакуемого сайта.

Устранение 4

Предпринять необходимые меры по ликвидации последствий инцидента.

Заменить измененный контент сайта на оригинальный, взятый из резервной копии. Убедиться в отсутствии уязвимостей в резервной версии сайта.

Восстановление 5

Восстановить систему до нормального состояния.

- **Поменять пароли всех пользователей.** Если у вас есть основания предполагать возможность компрометации авторизационных данных пользователей, обнулить все доступы с последующим оповещением пользователей.

- **В случае существования резервного сервера, восстановить все компоненты основного сервера за счет резервной копии.**

После инцидента 6

Задокументировать детали инцидента и собранную информацию, извлечь уроки, оптимизировать процессы защиты.

Оповещение

Если ситуация стала достоянием широкой общественности, оповестить пользователей о подробностях инцидента.

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

В случае обнаружения уязвимости, подробно задокументировать ее. В случае использования на сайте готового коммерческого решения, оповестить производителя ПО.

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 #6

Компрометация веб-ресурса (Defacement)

Реагирование на инциденты со скомпрометированными веб-сайтами

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**: 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.