Раздел: Жизненный цикл ИБ
Модуль: Методология анализа защищённости и вредоносное ПО
Выполнил: Александр Ганицев

Вводные данные
Компания ООО «АВС» — финансовая организация.

Руководитель — председатель правления Иванов А. Г.

Начальник отдела информационной безопасности — Петров Б. В.

У компании есть собственная SIEM-система (Security information and event management), т. е. система управления событиями безопасности.

В ООО «АВС» уже разработана политика управления инцидентами ИБ. Политика ссылается на отдельный низкоуровневый детализированный документ «План реагирования на инциденты ИБ».

Задание практической работы
Напишите план реагирования на инциденты ИБ для ООО «АВС».

В плане опишите порядок реагирования в общих случаях и, например, в виде отдельных порядков опишите реагирование на конкретные виды инцидентов, включая план реагирования на выявление вредоносного ПО.

План реагирования должен отвечать на следующие вопросы:

- Что делать в общем случае при выявлении инцидента?
- Что делать при выявлении конкретного инцидента: вредоносное ПО на серверах компании?

Итак, что нужно сделать по шагам:

1. Подумайте, кто или что может выявить инцидент в компании.
2. Опишите, кого должен уведомить этот сотрудник или система.
3. Определите, что должен сделать ответственный за дальнейшие действия сотрудник.
4. Определите, кто в каких случаях включается в рабочую группу.
5. Напишите план реагирования на инциденты ИБ для ООО «АВС».

Не зацикливайтесь на оформлении. Соответствие нормам оформления документов в задании не оценивается.

Условия реализации

Пришлите письменный отчёт в формате документа Microsoft Word или в формате PDF.

План реагирования может включать общую часть, верную для любой ситуации. Также в него могут входить отдельные планы для конкретных распространённых ситуаций: DDoS-атак,

выявления ВПО, утечки персональных данных, аномальной активности административной учетной записи и т. д.

План реагирования на инциденты ИБ для ООО «АВС»

Основные положения

1. Данный план расписывает меры, предпринимаемые для защиты цифрофой инфраструктуры компании “АВС”; последовательность шагов для купирования, ликвидации и восстановления систем; документирования, изучения и предотвращения их в будущем.

2. Любой инцидент произошедший на компьютерных системах компании есть тот внешний или внутренний фактор давления среды, который нельзя оставлять без внимания, и который, при должном проактивном мониторинге, реагировании и закрытии служит для создания более безопасной инфраструктуры компании и повышения уровня цифровой грамотности сотрудников и персонала ИТ инфраструктуры.

3. План применяется ко всем системам организации: серверам, рабочим станциям, мобильным и сетевым устройствам, а также локальным и подключённым к интернету (принтера, сканеры, специальные цифровые инструменты и т.д.).

4. Данный план составлен с учётом следующих документов:

- Федеральным законом “О защите персональных данных” № 152-ФЗ
- Федеральным законом “«Об информации, информационных технологиях и о защите информации" № 149-ФЗ»
- Постановлением Правительства РФ № 1119 «Об утверждении Правил разработки, утверждения и реализации планов реагирования на инциденты в области информационных технологий»;
- Межотраслевыми рекомендациями по обеспечению безопасности информации (МРБИ) - разработанные ФСТЭК России
- ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» - международным стандартом по управлению информационной безопасностью

5. Под инцидентом ИБ в данном Плане понимается событие вызванное внешним или внутренним воздействием на цифровые и электронные устройства компании перечисленные выше, при котором наносится ущерб самим устройствам или информации с целью компрометирования сотрудников компании и её клиентов, кражи важных данных и нарушения их целостности.
Инцидент ИБ наносит ущерб, способный нарушить течение процессов компании и привести к финансовым и репутационным потерям.

6. Основные виды инцидентов: остановка или вывод из строя компонентов системы, кража данных, кибератака (DDoS, вирус, ransomware, взлом электронной почты, spear/fishing-attack, получение административного доступа к важным компьютерным системам), методы социнжинерии для получения важной информации.

Организационная структура компании “АВС” при работе с инцидентами

Начальник отдела информационной безопасности Петров Б. В. разрабатывает политику работы с инцидентами внутри своего департамента и принципов взаимодействия с другими департаментами. В этом документе обозначены:
- Создание группы мониторинга и оперативного реагирования на инциденты
- Координация на всех этапах реализации данного Плана

Этапы работы с инцидентами

1. Подготовка компании.

1.1 Внедрение политики создания и ведения учётных записей всех сотрудников компании:

1.1.1 Сложные пароли, частота их смены, ведение журнала паролей

1.1.2 Многофакторная аутентификация

1.1.3 Процесс изменения прав доступа при смене роли сотрудника

1.1.4 Процесс немедленной деактивации учётных записей уволенных или ушедших сотрудников

1.2 Создание инфрастуктуры для выявления и анализа инцидентов:

1.2.1 Создание группы мониторинга и оперативного реагирования на инциденты:
- Назначение ответственных за различные компоненты инфраструктуры
- Выявление уровней опасности инциента: зелёный, оранжевый, красный
- Структурирование информирования связанных отделов и руководителей, указание лимита времени реагирования при обнаружении инцидента
- Создание реестра готовых сообщений для информирования сотрудников и клиентов компании

1.2.2 Мониторинг, обеспечение безопасности и аудит:
- Круглосуточный мониторинг всей инфраструктуры
- Внедрение SIEM системы
- Настройка прав журналирования и анализа событий
- Сканирование и внутренний аудит уязвимостей
- Проведение внутренних пентестов
- Проведение регулярного резервного копирования данных
- Внедрение централизованной системы антивирусной защиты

1.2.3 Регулярное обновление software и firmware компьютерного, сетевого оборудования и рабочих станций

1.2.4. Настройка безопасности сети:
- Защита всех компонентов сетевого оборудования
- Регулярная смена паролей
- Аудит настроек оборудования

1.3. Переодический инструктаж и обучение сотрудников затрагивающее все аспекты информационной безопасности:

1.3.1 Проведение трейнингов по Информационной Безопасности:
- ипспользование почты
- безопасное использование сети интернет, веб-ресурсов
- социальная инжинерия и телефонные мошенники
- защита ресурсов компании и воспитание ответственности на рабочем месте

1.3.2 Тестирование сотрудников посредством внутренних “атак” для выявления слабых мест в их информированности

1.3.3 Каждый сотрудник должен знать типы основных инцидентов и кого ему/ей необходимо уведомить в случае выявления

1.4 Проведение ежегодных сессий по Disaster Recovery и отработки взаимодействия с поставщиками оборудования и программного обеспечения.

1.5 Проведение аудита и пентеста специализированными компаниями.

1.6 Физическая защита сетевого и серверного оборудования.

2. Обнаружение и анализ

2.1 При обнаружении инцидента сотрудником (не ИТ специалист), он или она немедленно сообщают в письменном виде (почта) и посредством телефонного звонка в группу мониторинга и оперативного реагирования. Для этого у данной группы должна быть рабочий ящик электронной почты и выделенная телефонная линия. В письме кратко описывается ситуация и момент, когда она была обнаружена.

2.2. При обнаружении инцидента сотрудником ИТ департамента, он проведя своё краткое расследование, оценив риски и уровень инцидента, также уведомляет группу мониторинга и оперативного реагирования и оставаясь на месте продолжает аналитическуюработу над инцидентом.

2.3 Группа мониторинга и оперативного реагирования уведомляет вышестоящее начальство, анализирует инцидент.

2.4 Начальник отдела информационной безопасности выяснив степень серьёзности инцидента, и при ситуации, где есть возможность правовых последствий, репутационных потерь, уведомляет на экстренном совещании руководство компании, юридический отдел, отделы кадров, маркетинга и Public Relations.

2.5 Начальник отдела информационной безопасности приступает к коодинации процесса реагирования на инцидент и привлекает всех необходимых членов команды для работы.

3. Локализация, ликвидация и восстановление

3.1 Локализация:
- Изолируются системы подверженые воздействию
- Выявляется механизм воздействия и степень вредоносного воздействия
- Анализируются логи
- Данные об инциденте фиксируются в журнал инцидентов
- Инцидент классифицируется

3.2 Ликвидация:
- Обеспечиваются меры по нейтрализации и устранению инцидента
- Пеоверяются все системы, которые могут быть подвержены подобному воздействию

3.3 Восстановление:
- При необходимости системы возвращается к первоначальному состоянию
- Ползовательские данные восстанавливаются из резервных копий

4. Меры принимаемые после инцидента

4.1 Оформляется сводка по инциденту:
- Причины возникновения
- Нанесённый ущерб
- Принятые решения
- Последствия инцидента
- Итог расследования и восстановления
- Критичные данные заносятся в базу TI

4.2 Принимаются меры по предотвращению подобных инцидентов:
- Информирование сотрудников об инциденте
- Проведение сессий по ИБ для повышения уровня осознанности

План реагирования на инцидент типа выявления ВПО в инфомационной системе компании

1. Обнаружение и анализ

1.1 Обеспечение несения постоянного дежурства группы мониторинга и оперативного реагирования:

- Обеспечение ротации дежурного по реагированию, работу “горячей линии”
- Мониторинг 24/7 системы антивирусной защиты
- Регулярное обновление баз AV защиты и сканирование
- Проверка дежурным сотрудником версий баз в системе

1.2 Выявление ВПО:

- Анализ типа ВПО и оценка возможного урона

2. Локализация, ликвидация и восстановление

2.1 Локализация:

- Отключение скомпрометированной системы или систем от сети
- Анализ логов и событий

2.2 Ликвидация

2.2.1 Проведение мер по устранению ВПО:

- Предпринимается попытка нейтрализации угрозы
- По возможности сохраняются пользовательские данные

2.3 Восстановление:

- При серёзном ущербе системе она приводится к чистому состоянию
- Производится настройка всех элементов системы (сеть, периферийное оборудование, программное обеспечение)
- Данные восстанавливаются из резервных копий
- Пользователь проверяет и принимает систему

3. Меры принимаемые после инцидента

3.1 Сотруднику объясняются причины возникновения инцидента

3.2 Оформляется сводка по инциденту согласно основному Плану

3.2 Принимаются меры по предотвращению подобных инцидентов:

- Обновление баз AV всех систем
- Сканирование систем
- Информирование сотрудников