Тема доклада:
ШТАБНЫЕ КИБЕРУЧЕНИЯ

На фото: Учения на объекте
ООО «Газпром добыча Иркутск», 2021 год

ОБО МНЕ:

Самохвалов Семён, начальник отдела ИБ ООО «Газпром добыча Иркутск»

- С 2005 года занимаюсь защитой информации
- 8 лет в филиале Газпромбанка в г. Иркутске
- 8 лет в ООО «Газпром добыча Иркутск»
- Председатель государственной экзаменационной комиссии ИРНИТУ по направлению ИБ
- Организовал сообщество Ибэшники в Иркутской области

ПЛАН

1. Немного теории – 15 минут
2. Подготовка к учениям – 5 минут
3. Учения в группах – 50 минут
4. Подведение итогов – 10 минут
5. Вопросы – 10 минут

Итого: 1 час 30 минут

Теория

Для чего проводить учения?

ОСНОВАНИЯ ДЛЯ ПРОВЕДЕНИЯ УЧЕНИЙ:
Приказ ФСТЭК №239, п.13.6:
«б) обучение и отработка действий персонала по обеспечению безопасности значимого объекта в случае возникновения нештатных ситуаций; »

ОСНОВНАЯ ЦЕЛЬ: Объективная оценка действий персонала по обнаружению, предупреждению и ликвидации последствий компьютерных атак

Для чего проводить учения?

ЗАДАЧИ:

- Проверка эксплуатируемых средств и систем ИБ;
- Проверка работоспособности планов предупреждения и ликвидации последствий компьютерных атак.
- Совершенствование практических навыков ответственных лиц;
- Выявление темных пятен в подготовке специалистов;
- Формирование понимания последствий инцидентов;

Как действует злоумышленник?

Модель нарушителя

1. ВНУТРЕННИЙ ИЛИ ВНЕШНИЙ?
2. ПРИВИЛЕГИРОВАННЫЙ ИЛИ РЯДОВОЙ?
3. ПРОШЕЛ СПЕЦИАЛЬНУЮ ПОДГОТОВКУ ИЛИ СКРИПТ-КИДДИ?
4. СТРАТЕГИЯ И ТАКТИКА.

ИДЕАЛЬНО – рабочий кейс для демонстрации потенциала возможного развития атаки, без нанесения ущерба инфраструктуре.

Какие возможности для менеджера ИБ появляются при проведении учений?

ПЛЮСЫ ДЛЯ МЕНЕДЖЕРА ИБ:

1. ФОРМИРОВАНИЕ АДЕКВАТНОЙ КАРТИНЫ МИРА
2. НАЙТИ И УКРЕПИТЬ СЛАБОЕ ЗВЕНО
3. ПРОЯВИТЬ ОРГАНИЗАТОРСКИЕ СПОСОБНОСТИ
4. НАУЧИТЬ КОМАНДУ РАБОТАТЬ САМОСТОЯТЕЛЬНО
5. ВОВЛЕЧЬ РУКОВОДСТВО В ПРОЦЕСС

ИДЕАЛЬНО когда руководитель стоит в стороне и наблюдает за тем, как слаженно и без ошибок работает команда.

СЦЕНАРИЙ – ОСНОВА УЧЕНИЙ

ПРИМЕРНЫЙ СОСТАВ СЦЕНАРИЯ

1. ЛЕГЕНДА
2. ПОДГОТОВКА
3. ПЕРЕЧЕНЬ УЧАСТНИКОВ
4. ТАКТИЧЕСКАЯ ЧАСТЬ НАРУШИТЕЛЯ
5. ВЫЯВЛЕНИЕ И РЕАГИРОВАНИЕ
6. АНАЛИЗ ПОСЛЕДСТВИЙ И ИХ ЛИКВИДАЦИЯ
7. ПОДГОТОВКА ЦИФРОВЫХ УЛИК
8. ОТЧЕТНОСТЬ И РЕКОМЕНДАЦИИ

ВАЖНО заложить точное время для каждого этапа

ПРИМЕР СЦЕНАРИЯ – ПЛАНА УЧЕНИЙ

СОГЛАСОВАНО

Начальник Газового промысла

_____

« »_____ 2021

УТВЕРЖДАЮ

Главный инженер - первый заместитель генерального директора

_____

« »_____ 2021

П Л А Н
проведения тренировки по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак

г. Иркутск
2021

ПРИМЕР СЦЕНАРИЯ – ПЛАНА УЧЕНИЙ

На основании п. 7 Плана реагирования ….(утвержден приказом Общества …) и п. 5.1 Плана мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры Общества на 2021 год …, проводится тренировка по отработке взаимодействия подразделений, осуществляющих проведение мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

Тема: Взаимодействие работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры …. с персоналом значимого объекта критической информационной инфраструктуры ….., при возникновении компьютерных инцидентов, нацеленных на нарушение или прекращение функционирования объекта критической информационной инфраструктуры.

Дата проведения тренировки: «…» ….. 2021 года.

Время: с 15:00 до 16:00 (Иркутское время).

Место проведения: …...

Цели и задачи:

1. Совершенствование навыков и действий группы реагирования на инциденты информационной безопасности (определена Приказом ….).
2. Проверка исполнения схемы оповещения и алгоритма действий группы реагирования на инциденты информационной безопасности и работников …..
3. Отработка действий, предписанных Планом реагирования на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак ….

Подготовительные мероприятия:

1. Выделение мобильного устройства (ноутбук) для использования в качестве оборудования потенциального злоумышленника.
2. Изменение DNS-имени, MAC-адреса оборудования потенциального злоумышленника на период проведения тренировки для симуляции стороннего (нештатного) оборудования.

ПРИМЕР СЦЕНАРИЯ – ПЛАНА УЧЕНИЙ

Этап действий	Действия персонала	
	1. Реагирование на инцидент	
1.1.	**ДО**: замечает срабатывание сигнализации шкафа «на открытие» с оборудованием системы … на Позиции. Оператор уведомляет **АСА.** Время исполнения : (чч:мм)	
1.2.	**АИБ СА** фиксирует, что системой мониторинга событий информационной безопасности зафиксированы события в сети … *(подключение мобильного устройства злоумышленника в сети ...).* Время исполнения __:__ (чч:мм)	
1.3.	**АИБ СА**: замечает срабатывание системы антивирусной защиты на сервере системы управления … с оповещением о сетевой атаке *(активное сканирование портов злоумышленником).* Время исполнения : (чч:мм)	
1.4.	**АИБ СА**: незамедлительно информирует о происшествии РО, ОИБ СКЗ. Время исполнения : (чч:мм)	
1.5.	**ОИБ СКЗ**: принимает поступившую информацию, совместно с **АИБ СА** производит оценку сообщений средств защиты информации, выясняет обстоятельства происшествия. Время исполнения __:__ (чч:мм)	**РО**: принимает поступившую информацию. Дает команду **АСА** по проверке функционирования Системы управления; Время исполнения __:__ (чч:мм) **АСА**: проверяет работоспособность …, направляет представителя на Позицию для проверки, докладывает **РО** о проведенной проверке. Время исполнения : (чч:мм)
1.6.	**ОИБ СКЗ**: замечает срабатывание системы корреляции событий информационной безопасности (SIEM) на подбор пароля к Серверу. Время исполнения __:__ (чч:мм)	
1.7.	**ДО**: замечает неисправность в системе управления технологическими процессами (Сервер не отвечает). Оператор уведомляет **АСА.** Время исполнения : (чч:мм)	
1.8.	**ОИБ СКЗ**: немедленно докладывает **Ру ГРИИБ** (по телефону). Время исполнения __:__ (чч:мм)	**РО**: дает команду **АСА** на передачу управления резервному контуру АСУ ТП. Время исполнения __:__ (чч:мм) **ДО**: приступает к выполнению должностных обязанностей на резервном контуре Системы управления

ШТАБНЫЕ КИБЕРУЧЕНИЯ

УЧЕНИЯ (ФАЗА 1 - подготовка)

1. КРАТКОЕ ОПИСАНИЕ ОРГАНИЗАЦИИ:

   Активно развивающийся региональный банк с ориентиром на потребительское кредитование и брокерское обслуживание.

2. ПОДГОТОВКА (5 МИНУТ)

   - Распределиться по группам
   - Дать название команде – организации

ВЕДИ ЧЕК-ЛИСТ ИНСАЙТОВ

УЧЕНИЯ (ФАЗА 1 - подготовка)

ЗАДАЧА – ПРИДУМАТЬ КЕЙС ДЛЯ УЧЕНИЙ (5 - 10 МИНУТ)

ВАЖНО - Вовлечь всех участников команды - раздать роли.

Примерный состав возможных участников:

ГД, ЗГД, отдел ИБ, отдел связи, отдел ИТ, helpdesk, служба СМИ, отдел по работе с корпоративными клиентами, фронт и бэк офис, секретариат, юристы и др.

УЧЕНИЯ (ФАЗА 2 - тренировка)

1. ПОДГОТОВИТЬ СЦЕНАРИЙ (10 МИНУТ)

- ЛЕГЕНДА
- ПОДГОТОВКА К УЧЕНИЯМ
- ПЕРЕЧЕНЬ УЧАСТНИКОВ
- ТАКТИЧЕСКАЯ ЧАСТЬ НАРУШИТЕЛЯ
- ВЫЯВЛЕНИЕ И РЕАГИРОВАНИЕ
- АНАЛИЗ ПОСЛЕДСТВИЙ И ИХ ЛИКВИДАЦИЯ
- ПОДГОТОВКА ЦИФРОВЫХ УЛИК

2. ГРУППОВОЙ АНАЛИЗ СЦЕНАРИЕВ (10 МИНУТ)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО

УЧЕНИЯ (ФАЗА 3 – анализ и реагирование)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО (5-10 МИНУТ)

КЕЙС №1

Вы развернули пилот системы предотвращения утечек информации (DLP). В целях исключения возможных сбоев не стали настраивать систему на работу в режиме перехвата, оставили работать в режиме мониторинга. Утром, на следующий рабочий день в логах вы обнаружили что менеджер организации направил себе на личную электронную почту персональные данные 6 клиентов.

Опишите подробно ваши действия.

2020 г. – Андрей Одоев, работая в Альфа-Банке, передал данные 6 клиентов банка мошенникам из Москвы. Данные были использованы преступниками для изготовления фальшивых паспортов и открытия банковских карт.

В результате **с трёх счетов украли** **более 8,5 млн рублей**. За свою «помощь» сотрудники банка получили **по 70 тысяч рублей каждый.**

Одоев был признан судом Архангельска виновным и обязал его выплатить 50 тыс. руб. в качестве наказания.

УЧЕНИЯ (ФАЗА 3 – анализ и реагирование)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО (5-10 МИНУТ)

КЕЙС №2

На следующий день во время утреннего кофе, просматривая сообщения, полученные ночью, вы натыкаетесь на смс от своего знакомого примерно следующего содержания:«Вас что, действительно взломали?» Учитывая часовую разницу, вы понимаете, что тревожить знакомого сейчас некультурно.

Опишите подробно ваши действия.

УЧЕНИЯ (ФАЗА 3 – анализ и реагирование)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО (5-10 МИНУТ)

КЕЙС №3

В этот же вечер, после 22.00 вам начинают поступать сообщения от технической поддержки что ИТ-инфраструктура организации работает нестабильно, некоторые файлы перестают открываться и превращаются в сердечки, появляются дополнительные файлы.

Опишите подробно ваши действия
с привязкой к временным интервалам

8 марта американский разработчик Брэндон Нозаки Миллер выложил на GitHub пакеты ПО с открытым исходным кодом с названиями Peacenotwar и oneday-test.

Пользователи заметили, что некоторые последние обновления популярной библиотеки node-ipc, также поддерживаемой этим разработчиком, запускают вредоносный код, удаляющий все данные с компьютера.

Скрипт определял IP-адрес и, если пользователь оказывался из России или Белоруссии, удалял их данные, заменяя на эмодзи сердца.

УЧЕНИЯ (ФАЗА 3 – анализ и реагирование)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО (5-10 МИНУТ)

КЕЙС №4

Вы находитесь в ресторане и празднуете день рождения жены, когда раздается звонок от вашего руководителя, который рассказал что ему позвонил Генеральный директор и сообщил, что его домашний ноутбук на Windows зашифрован. Он принес его на работу, вызвонил вашего руководителя и попросил его разобраться – решить проблему. Ваш руководитель делегирует эту задачу вам.

Автор – Алексей Лукацкий

УЧЕНИЯ (ФАЗА 3 – анализ и реагирование)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО (5-10 МИНУТ)

КЕЙС №5

В течение суток с момента заражения личного ноутбука генерального директора отдел ИБ не смог восстановить доступ к данным (резервная копия отсутствует) и генеральный директор позвонил вам и потребовал оплатить выкуп вымогателям, так как на ноутбуке находится ценная информация (архив фотографий детей с момента их рождения).

Автор – Алексей Лукацкий

УЧЕНИЯ (ФАЗА 3 – анализ и реагирование)

АНАЛИЗ КЕЙСОВ ОТ ВЕДУЩЕГО (5-10 МИНУТ)

КЕЙС №6

Злой Админ

Сразу после новогодних праздников один из администраторов ИТ-инфраструктуры сообщает о своем увольнении. Вы наслышаны о его конфликте с руководителем организации накануне. Работник не планирует отрабатывать 14 дней и требует выдать ему трудовую книгу сегодня.

Опишите подробно ваши действия.

ПОДВЕДЕНИЕ ИТОГОВ

ВЫВОДЫ

1. ВАЖНО ПРОВОДИТЬ ШТАБНЫЕ КИБЕРУЧЕНИЯ
2. НУЖНО РАЗРАБАТЫВАТЬ СЦЕНАРИЙ
3. ВОВЛЕКАТЬ В ПРОЦЕСС УЧЕНИЙ РУКОВОДСТВО
4. НАБЛЮДАТЬ СО СТОРОНЫ ЗА ПРОИСХОДЯЩИМ
5. ТРЕНИРОВАТЬСЯ НЕ РЕЖЕ 1 РАЗА В ГОД
6. ФИКСИРОВАТЬ ТАЙМИНГ ВСЕХ ШАГОВ
7. ДЕЛАТЬ ВЫВОДЫ И РАЗБОР ПО РЕЗУЛЬТАТАМ УЧЕНИЙ
8. АКТУАЛИЗАЦИЯ "ЭКСТРЕННЫХ ПЛАНОВ"

Спасибо за внимание!

Готов ответить
на ваши вопросы

Моя визитка

Мои контакты:
Телефон: 89021772542
Telegram: @Samohvalov
Vk.com\samohvalov_sa