SOLAR

КИБЕРПОЛИГОН

ЧЕК-ЛИСТ ПО ПРОВЕДЕНИЮ КИБЕРУЧЕНИЙ

Что делать до киберучений?

Что делать во время киберучений?

Что делать после киберучений?

W: RT-SOLAR.RU

T: +7 (499) 755-07-70

1. Определить цель

Сформулируйте однозначные, понятные для всех участников цели проведения киберучений

2. Определить состав участников

01 Для кого проводим киберучения?
- топ-менеджмент
- инженерный персонал
- административный персонал

02 Сколько будет участников?

03 Какие навыки необходимы участникам?

04 Как будет происходить набор участников?
- конкурсный отбор
- списки от руководителей
- заявки от всех желающих

3. Выбрать тип учений

Публичные
или внутрикорпоративные

Практические
(с отработкой
на инфраструктуре)

Теоретические
(брейншторм)

Как будут подключаться участники — очно, онлайн, и так и так?

Место проведения: свой офис или внешняя площадка?

4. Разработать механику киберучений

01 Какой формат киберучений?

- Capture the Flag
- Red vs Blue
- отработка взаимодействия
  (команды взаимодействуют между собой либо с координационным центром, CERT или SOC)

02 Каким образом будут осуществляться кибератаки, в ручном (Red Team) или автоматизированном формате?

03 Как будут взаимодействовать участники между собой и внутри команд?

04 Какие цели стоят перед участниками? Какие будут этапы?

5. Подготовить инфраструктуру для проведения киберучений

01 На какой инфраструктуре проводятся киберучения:

- на цифровом двойнике
- на реальной инфраструктуре?

02 Какие основные инфраструктурные элементы (серверы, приложения и специализированное ПО, устройства промышленной автоматизации и т. д.) будут применяться?

03 Каков состав средств защиты информации, применяемых в рамках киберучений. Насколько средства защиты информации и их конфигурация соответствуют используемым в вашей инфраструктуре?

04 Какой легитимный трафик должен быть в инфраструктуре? Определите формат воспроизведения трафика:

- ручной
- автоматизированный
  (он требует соответствующих скриптов или инструментов генерации)

05 Как будет восстанавливаться инфраструктура в случае сбоев

06 Какие сервисы будут применяться для коммуникации с участниками (почта, мессенджеры и др.)?

6. Продумать скоринг

01 Каким образом (автоматические чекеры, вручную) и за какие задания будут начисляться баллы?

Скоринг должен быть непротиворечивым и логичным: при необходимости скорректируйте «вес» различных заданий в зависимости от их сложности

02 Какие навыки будут проверяться в ходе киберучений и какие метрики будут для этого использоваться?

03 В случае соревновательного формата: пропишите условия победы, поражения и начисления или снятия дополнительных баллов

В дальнейшем эти условия должны быть доведены до участников в ходе брифингов и включены в «Руководство участника»

7. Подготовить справочную документацию

Опишите правила, цели и задачи киберучений в «Руководстве для участников»

Четко пропишите запрещенные действия и ограничения. Укажите перечень специализированного ПО и средств защиты информации, которые могут использовать участники

Разработайте карту коммуникаций участников: с кем взаимодействуют команды (другие участники, CERT/SOC, координационный центр и т. д.)

Для территориально распределенных учений пропишите каналы связи (электронная почта, мессенджеры, Discord и т. д.)

Разработайте тайминг мероприятия (сценарий событий, дедлайны по задачам участников и т. д.)

При необходимости разработайте «Руководство для организаторов» (это пригодится для масштабных учений, где требуется координация большого числа событий)

Сформируйте сжатые тезисы брифингов для участников — они проводятся перед стартом учений и в ходе игровых событий

Их можно дополнять — при возникновении технических ограничений на площадке, изменении состава участников и т. д.

8. Обеспечить маркетинговую и PR-поддержку

(для публичных киберучений)

01 Продумайте, как сделать киберучения интересными для зрителей

- визуализация атак
- соревновательные элементы
- спецэффекты

02 Заранее согласуйте с участниками допустимость упоминания их в пресс-релизах и публикациях

03 Заложите бюджет на призы участникам киберучений

9. Провести тестирование киберучений

01 Разверните инфраструктуру, планируемую использовать в рамках киберучений

02 Проведите проверку сформированных механик на тестовой группе

03 Рассмотрите реализуемость и прозрачность скоринга

04 Рассмотрите актуальность и достаточность справочной документации

05 Соберите обратную связь по итогам тестирования и внесите необходимые корректировки

10. Прописать риски

Выпишите и проанализируйте все возможные риски (даже маловероятные), ранжируйте их по вероятности возникновения

Пропишите риски, которые невозможно митигировать действиями организаторов:

- отказы команд от участия
- изменение политической обстановки и т. д.

ПРОДУМАЙТЕ «ПЛАН Б» НА СЛУЧАЙ ЭКСТРЕННЫХ СИТУАЦИЙ

11. Контролировать ход мероприятия

01 Используйте «внутриигровые» сообщения, чтобы контролировать ход учений

- электронные письма
- сводки новостей
- объявления модератора и т.д.

02 Следите за таймингом: корректируйте ход мероприятия, если участники не укладываются в отведенное время либо справляются слишком быстро

03 Продумайте подсказки и механизмы усложнения заданий — это потребуется, если уровень участников окажется выше или ниже того, на который вы ориентировались при подготовке

12. Помогать участникам

Проследите, чтобы модераторы своевременно помогали участникам, отвечали на вопросы во всех каналах коммуникации

Организуйте и контролируйте работу технической поддержки, проследите, чтобы операторы 1-й линии оперативно отвечали на технические вопросы участников

13. Быть готовым к неожиданностям

Продумайте, как и чем вы будете занимать участников в случае непредвиденных технических или организационных проблем или сбоев (например, отключения интернета)

14. Использовать обратную связь

01 Соберите фидбек с участников — предложите заполнить им небольшой опросник

02 Дайте участникам обратную связь в виде отчета — он может включать рекомендации по оптимизации процессов обеспечения ИБ, взаимодействия между подразделениями и т. д., а также обзор киберучений:

- сколько заданий выполнили участники
- какие верные и неверные действия совершили и т. д.

03 Хорошая практика — сделать два отчета:

- сжатый (основные выводы, тезисы и рекомендации) для руководства
- развернутый технический для ИБ-специалистов

15. Провести ретроспективный анализ мероприятия

Проанализируйте результаты опроса участников

Проведите сессию в формате «Что было сделано хорошо? Что было сделано плохо?»

Систематизируйте и задокументируйте результаты разбора для использования в качестве базы знаний при проведении киберучений в дальнейшем

SOLAR

W: RT-SOLAR.RU
W: RT.RU

+7 (499) 755-07-70
solar@rt-solar.ru

Центральный офис, 125009,
Москва, Никитский переулок, 7с1