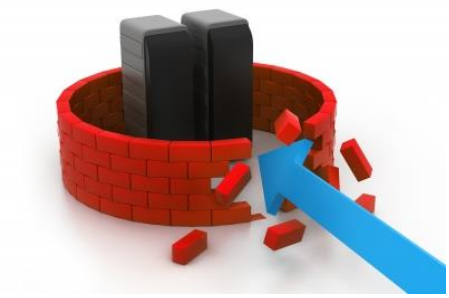
SecurityLab.ru
by Positive Technologies

Red Team и Penetration Test vs Киберучения. Наш подход

Издание: SecurityLab.ru, 15 мая 2018 г.

Спикер: Игорь Мотрони, ведущий эксперт отдела анализа защищенности компании «Информзащита»



К сожалению, даже самые навороченные системы защиты не делают вашу инфраструктуру абсолютно безопасной.

Вместо предисловия

На сегодняшний день у всех людей, так или иначе связанных с информационной безопасностью, на слуху термины Red Team, APT, CERT и SOC. Сфера развивается невероятно стремительно, и системы обеспечения ИБ многих компаний достигли такого уровня зрелости, когда обычные тесты на проникновение перестают приносить ощутимые результаты, кроме выполнения требований и контроля ошибок вроде пропущенного обновления безопасности или некорректной конфигурации свежего ПО.

В этот момент возникает вопрос: что дальше?

Red Team и Penetration Test

Не буду заново разжевывать эту тему, количество статей в Интернете о данном сравнении измеряется десятками. Принято считать, что дальше компании следует организовать отдельную команду специалистов, задача которых будет заключаться в непрерывных атаках на инфраструктуру организации.

Основные отличия от обычного тестирования посредством черного ящика:

• специалисты знают, что и как устроено в организации и где могут встретиться потенциальные уязвимости. Они в курсе о происходящих изменениях в ИТ-инфраструктуре и им легче оказаться «в нужное время в нужном месте»,

• изначально отсутствуют какие-либо ограничения на область работ,

• они могут проводить атаки в любое время дня и ночи без предварительного предупреждения.

Собственно, как и в реальной жизни. Однако надо понимать, что и Red Team не идеален: во-первых, для постоянного «стресс-тестирования» службы ИБ необходимо содержать отдельную команду offensive-специалистов, а это удовольствие не из дешевых.

Во-вторых, кропотливая работа в рамках Red Team-проектов занимает длительное время, причем значительная его часть тратится на то, чтобы избежать так называемого «шума» в трафике.

Киберучения

В качестве одного из решений сложившейся ситуации с тренировкой сотрудников службы ИБ в «боевых» условиях «Информзащита» предлагает организовывать Киберучения. Зачем тратить время и деньги на преодоление технических средств, если вы хотите защититься от злоумышленника, имеющего доступ к 0day-уязвимостям и техникам проникновения, еще не попавшим в сигнатурные базы средств защиты?

Кому они нужны? Киберучения следует проводить организациям с высоким уровнем зрелости системы ИБ. Одним из индикаторов требуемого уровня являются стабильно положительные результаты регулярных тестирований на проникновение (отсутствие уязвимостей с высоким и средним уровнем риска, высокий уровень общей защищенности).

В таком случае можно сказать, что инфраструктура организации защищена от публично известных атак. Однако статистика показывает, что большая часть ущерба наносится в результате целевых атак (APT), использующих т.н. уязвимости «нулевого» дня, эксплуатацию которых невозможно предотвратить. При таких атаках решающую роль будет играть готовность службы ИБ оперативно реагировать на возникающие инциденты, а также наличие средств для выявления проводимой таргетированной атаки.

Многие компании на сегодняшний день активно внедряют anti-APT решения, такие как песочницы и ханипоты, однако фактически протестировать они их могут только во время реальной APT-атаки, где шанса на ошибку уже не будет. Обычный тест на проникновение не подразумевает тестирование защитных средств, поэтому подобную потребность вполне можно удовлетворить с помощью Киберучений.

Киберучения позволяют:

- выявить потенциальные вектора проникновения в инфраструктуру;
- провести стресс-тест сотрудников отдела по реагированию на инциденты и отдела ИБ;
- «дать почувствовать» хакерскую атаку людям, далеким от аспектов информационной безопасности (фишинговые рассылки и т.д.)
- протестировать технические средства выявления и предотвращения хакерских атак.

Кстати, не всегда такие учения нужно организовывать самостоятельно. Например, международный форум по безопасности Positive Hack Days уже в третий год проводит кибербитву The Standoff, которая по своей сути является киберучениями. Здесь в 30-часовой период укладываются сценарии атак, которые в реальной жизни растягиваются на дни и недели, в числе атакующих оказываются специалисты с различным уровнем подготовки (от супер-профи до любителей). Благодаря этому можно на практике отработать реагирование на различные сценарии атак, протестировать используемые инструменты в полевых условиях и, конечно, же организовать для своих экспертов тестирование в условиях массированных атак.

Варианты реализации

Full-scope penetration test

«Продвинутое» комплексное тестирование на проникновение. Выполняется следующими этапами:

1. Обычный комплексный тест на проникновение.

2. Составление списка потенциальных сценариев атак на основе полученной информации и согласование проводимых атак с заказчиком.

3. Симуляция согласованных атак (без сообщения службе ИБ).

4. Разбор результатов.

Непрерывное тестирование

Постоянная симуляция различных атак (также при согласовании и без уведомления службы ИБ) на основе каких-либо SLA. С предоставлением отчетов на регулярной основе.

Симуляция атак

Здесь согласование и симуляция атак проходят без предварительного тестирования. Необходимый доступ (в зависимости от выбранной атаки) предоставляется организацией-заказчиком.

Сценарии атак

В качестве сценариев различных атак, которые можно использовать для проверки реального состояния системы обеспечения ИБ (не только технических решений, но и процессов и сотрудников), можно использовать следующие примеры:

· компрометация какого-либо внешнего узла (удаленное исполнение произвольного кода на одном из узлов, например, web-сервере и развитие атаки вглубь организации);

· инсайдерская атака (из пользовательского сегмента, с дополнительными знаниями инфраструктуры);

· атака из гостевой wi-fi - сети (при условии «пробития”» разграничений доступа, при их наличии);

· физическое хищение имущества (хоть это и не находится в рамках кибербезопасности, такие сценарии атак вполне реальны, и их тоже имеет смысл рассматривать);

· социальная инженерия (данное упражнение мы часто проводим и в рамках тестов на проникновение, однако при симуляции реальной атаки нагрузки, передаваемые с письмами, направлены на первичное закрепление на компьютере жертвы и дальнейшее развитие атаки вглубь сети организации);

· DoS / DDoS-атака на какой-либо внешний сервис (данная атака находится под большим вопросом и очень сильно зависит от цели и возможностей потенциальных заказчиков).

Вывод

К сожалению, даже самые навороченные системы защиты не делают вашу инфраструктуру абсолютно безопасной.

Процессы и уровень готовности персонала к кибератакам должен иметь хороший технический тыл, поэтому обучение и тренировки следует проводить не на словах, а в условиях, идентичных реальным атакам, которые позволят быстро выявить пробелы и проблемы в актуальном состоянии вашей системы ИБ.

Подробнее: https://www.securitylab.ru/phdays/articles/493277.php