Практическое задание. Защитные механизмы.

Рекомендуемые средства защиты информации и меры, для нейтрализации возможной компьютерной атаки, согласно этапов матрицы MITRE

1. Разведка.
Для усложнения этого этапа можно использовать системы IDS/IPS, которые будут оповещать и предотвращать подозрительную активность, например Snort, также для защиты веб-ресурса можно использовать WAF, Positive Technologies Application Firewall

2. Подготовка ресурсов.
Для усложнения действий злоумышленников на данном этапе, необходимо чёткое понимание используемых компонентов информационной системы и своевременное обновление их, перекрывающее выявленные уязвимости. Использовать сканеры уязвимостей. Необходимо проводить обучение сотрудников по вопросам кибергигиены и важности использования сложных паролей, недопустимости использования одинаковых паролей, чаще их менять, строго разделять личные и рабочие учетные записи. Должны быть созданы регламенты, инструкции, политики, в которых это будет всё закреплено.

3. Первоначальный доступ.
Во избежание использования уязвимости сайта и попадания злоумышленников во внутреннюю сеть компании, необходимо предусмотреть DMZ (демилитаризованная зона), которая будет выступать буфером, затрудняя проникновение. Проводить обучение и тренинги персонала. Осведомленность сотрудников о вариантах фишинга и методах социальной инженерии перекроют часть путей к первоначальному несанкционированному доступу к системам. Необходимо использовать межсетевые экраны (Firewall) для контроля входящего и исходящего трафика, это могут быть встроенные брандмауэры в ОС, либо же отдельные решения, как программные, так и аппаратные. Например: Iptables, Континент 4 (Код Безопасности).

4. Выполнение.
Использовать антивирусную защиту, например, решения от Лаборатории Касперского, что затруднит выполнение большой части вредоносных действий. Использовать EDR для защиты информации на конечных устройствах, например, Kaspersky EDR.

5. Закрепление.
Плановое регулярное сканирование всей информационной инфраструктуры компании на наличие вредоноса, например, решения от Лаборатории Касперского. Контроль логов. Использовать Snort в качестве ids/ips решения для выявления и предотвращения попыток закрепиться.

6. Повышение привилегий.
На данном этапе поможет использование двух факторной аутентификации, использование PAM системы SafeInspect, для управления привилегированным доступом. Разделение сетей.

7. Предотвращение обнаружений.
Использовать IDS/IPS, можно использовать NGFW решение, например, UserGate NGFW. Плановое регулярное сканирование инфраструктуры. Мониторинг событий безопасности для обнаружения подозрительной активности.

8. Получение учётных данных.
На данном этапе поможет бдительность сотрудников, полученная во время обучения. А также система IDS/IPS, например, Snort.

9. Исследование.
Этому будут препятствовать системы обнаружения и предотвращения сетевых вторжений (IDS/IPS). Можно предусмотреть системы ресурсов-приманок (“муляжи” информационных систем)

10. Перемещение внутри периметра.
Здесь поможет разделение сети на сегменты с разными уровнями доступа, межсетевые экраны. Для анализа сетевого трафика и выявления необычной активности подойдет СЗИ NTA Гарда Монитор.

11. Сбор данных.
Шифровать данные при передаче и хранении для защиты конфиденциальной информации. Использовать СЗИ от НСД Dallas Lock.

12. Управление и контроль.
Отслеживаем неспецифический для организации исходящий и входящий сетевой трафик. Полезным будет NGFW решение UserGate NGFW.

13. Эксфильтрация данных.
Поможет запрет на загрузку в облачные хранилища, создание белого списка интернет ресурсов, доступных из корпоративной сети компании. Отслеживать неспецифический для организации трафик. Ограничить размер передаваемых блоков данных. Можно использовать PT NAD, который постоянно мониторит сетевой трафик и поэтому способен обнаруживать эксфильтрацию данных и соединения вредоносного ПО с командными серверами.

14. Воздействие
Для минимизации негативных последствий, сохранения информации и быстрого восстановления работоспособности ресурсов, необходимо регулярно делать бэкапы. Для этого можно использовать системы резервного копирования RuBackup.
PT Application Firewall может предотвращать дефейс веб-сайтов, доступных извне корпоративной сети.