Защитные механизмы.
Нейтрализация 14-ти этапов атаки по матрице MITRE.

Учитываем особенности IT инфраструктуры - коммерческая организация, которая занимается грузоперевозками. В организации работают отделы:

1. Менеджеры по грузоперевозкам;
2. Бухгалтерия;
3. Кадровая служба;
4. Служба ИТ.

IT инфраструктура была устроена таким образом:
- сайт, размещённый на собственных мощностях;
- DMZ-зона отсутствует;
- удалённых сотрудников нет;
- менеджеры звонят с использование IP-телефонии.

1. Разведка

1.1. Создаём DMZ зону, в которую выносится веб-сайт, почтовый сервер и IP-телефония организации. Сетевая структура разделяется на две подсети: внутреннюю и DMZ, для усложнения возможности взлома и получения несанкционированного доступа к ресурсам организации.

1.2. На обоих брэндмауэрах закрываем порт 445 для входящих соединений.

1.3. Взаимодействуем только с разрешенными адресами, вводим контроль по IP или MAC адресам.

1.4. Устанавливаем доступ к международной связи только для сотрудников, которым она необходима. Список сотрудников строго коррелируется с новыми/уходящими сотрудниками. В обязательства сотрудников техподдержки входит настройка и блокирование доступа к IP телефонии (равно и других учётных записей) в организации (найм, временное отстранение от службы, увольнение, долгий отпуск по болезни и т.д.).

1.5. Отслеживаем подозрительный сетевой трафик, который может указывать на:
- проверку адресов электронной почты и/или имен пользователей;
- сканирование IP-адресов;
- большое и/или повторяющееся количество запросов на аутентификацию, исходящих из одного источника.

1.6. Анализируем веб-метаданные и сайт организации для выявления артефактов, которые можно отнести к потенциальной уязвимости.

2. Подготовка ресурсов.

2.1. Все компоненты информационной системы организации обновляются до последних доступных версий: серверные и клиентские ОС, специализированное ПО, firmware брэндмауров, коммутаторов, принтеров и прочего оборудования.

2.2. Для всех сотрудников организации планируются и проводятся курсы и образовательные лекции на тему информационной безопасности.

2.4. Сотрудники обязаны жёстко разделять личные учётные записи и все остальные, связанные с работой. Все почтовые учётные записи, различные публичные и облачные эккаунты переводятся на 2ФА.

3. Первоначальный доступ.

3.1. Изолировать приложения и ограничить доступ к другим процессам и функциям системы, к которым может получить доступ эксплуатируемая цель.

3.2. Регулярно сканировать внешние системы на наличие уязвимостей и устанавливать процедуры для быстрого исправления систем при обнаружении критических уязвимостей.

3.3. Регулярно проверять учетные записи пользователей на предмет активности.

3.4. Настроить политику условного доступа, чтобы блокировать вход в систему с несовместимых устройств или с IP-адресов, находящихся за пределами определенных диапазонов IP-адресов организации.

3.5. Установка антивируса и систем, предназначенные для сканирования и удаления вредоносных вложений электронной почты.

3.6. Обучение пользователей распознавать методы социальной инженерии и целевые фишинговые электронные письма.

4. Выполнение.

4.1. Отслеживание выполняемых команд и аргументы для действий, которые используются для удаленного выполнения.

4.2. Настраивается и поддерживается средство для мониторинга веб-трафика и блокирования атак на веб-приложения.

4.3. Настраиваются файерволы UserGate NGFW или Check Point NGFW для внешнего периметра и подобный NGFW или Ideco UTM решения для внутреннего барьера защиты.

5. Закрепление.

5.1. Сотрудники IT отдела планово проводят сканирование всех систем организации на наличие rootkit, вирусов, червей, malware, adware, и прочих вредоносных программ.

5.2. Провести проверку выполненных команд и аргументов в истории команд, либо в консоли, либо в оперативной памяти, чтобы определить, использовались ли несанкционированные или подозрительные команды для изменения конфигурации устройства.

5.3. Постоянно отслеживать изменения, внесенные в механизмы загрузки до ОС.

5.4. Контроль за вновь созданными сетевыми подключениями.

6. Повышение привилегий.

6.1. Для предотвращение повышения привилегий при взломе системы, или первоначальном проникновении злоумышленников, необходимо приобрести, настроить и проводить круглосуточный мониторинг состояния SIEM системы.

6.2. Необходимо настроить IDS/IPS: HIDS – OSSEC и NIDS – Snort.

7. Предотвращение обнаружений.

7.1. Плановый мониторинг всей инфраструктуры организации посредством SIEM и IDS/IPS системы.

7.2. Плановый мониторинг антивирусного барьера.

8. Получение учётных данных.

8.1. Проверить и настроить шифровку всего проводного и/или беспроводного трафика.

8.2. Проводится hardening AD домена.

8.2. Настраиваются политики учётных записей (создание, заморозка, деактивация, удаление, лишение доступа, ограничения доступа).

8.3. Проведение регулярных сессий с пользователями компьютерных систем. Повышаем бдительность сотрудников к приходящим почтовым сообщениям, звонкам, объясняем принципы социальной инжинерии. Даём советы по обеспечению профессиональной и личной информации.

9. Исследование.

9.1. Предотвращаем любые попытки вторжения, аномальных обращений к объектам сетевой инфраструктуры организации посредством мониторинга систем обнаружения SIEM.

9.2. Предотвращаем попытки вторжения поредством вирусов, звонков и установки устройств для снятия информации. В процессе разрастания инфраструктуры организации рассматриваем возможности масштабирования процессов ИБ.

9.3. Исследуем все системы на наличие потенциальных уязвимостей посредством сканеров уязвимости, рассмотреть следующие продукты.

10. Перемещение внутри периметра.

10.1. Постоянное обновление ПО, firmware для всех элементов инфраструктуры.

10.2. Периодическая смена паролей.

10.3. При необходимости, для ключевых систем в финансовом отделе, для доступа к важным приложениям, используем комбинацию 2ФА и OTP.

10.4. Мониторинг аномальной активности учётных записей, вне обычных временных режимов работы, смены паролей, добавления новых систем в домен, и т.д.

10.5. Одним из важнейших компонентов поддержания системы в нормальном состоянии, создаём и поддерживаем систему резервного копирования.

11. Сбор данных.

11.1. Вырабатываем методы распознавания сниффинг и спуффинг атак. Повышаем бдительность сотрудников. Определяем вознаграждение при выявлении подобного инциента.

11.2. Используя DLP решение, выявляем нестандартную активность сотрудников и принимаем меры.

12. Управление и контроль.

12.1. Используя SIEM систему, отслеживаем неспецифический для организации исходящий и входящий сетевой трафик, исследуем пакеты, в которых может маскироваться управленческая деятельность злоумышленников.

12.2. В своей сети ведём чёткую инвентаризацию всех существующих хостов и систем, при добавлении новых, расследуем и действуем.

12.3. Для предотвращения утечки информации и нанесения организации ущерба вырабатываем процедуры отрезания сети от внешнего мира для скорейшего восстановления работоспособности всех поражённых систем. Тщательным образом проверяем всю инфраструктуру перед подключением в сеть Интернет.

13. Эксфильтрация данных.

13.1. Действия схожи с пунктом 12.

14. Воздействие.

Рассмотреть возможность реализации плана аварийного восстановления информационной структуры. Должен содержать процедуры для регулярного создания резервных копий данных, которые можно использовать для восстановления данных организации.

Убедиться, что резервные копии хранятся вне системы и защищены.