Риск-менеджер

Стажировка в VK

Вопрос 1

Группа Carbank использует для своих атак ряд техник представленных по ссылке (https://attack.mitre.org/groups/G0008/)

Подберите набор контролей из CIS18 (https://www.cisecurity.org/controls/cis-controls-list), способных снизить вероятность эксплуатации этих техник (вы можете использовать раздел mitigations в MITRE). В качестве результата представьте график и/или сводную таблицу (используйте функцию pivot table excel), отображающую какую из функций СУИБ (из NIST CSF) необходимо улучшать в первую очередь для защиты от Carbank.

По желанию вы можете представить дополнительную аналитику из сформированных данных, которая может помочь принять решение об инвестициях в ИБ.

Ответ:

Основываясь на матрице Mitre ATT&CK для группы Carbank, следующие элементы управления CIS могут использоваться для снижения вероятности использования этих методов:

1. Контроль 1 — Инвентаризация и контроль аппаратных активов: помогает идентифицировать все аппаратные активы и предотвращает несанкционированный доступ к этим устройствам.

2. Контроль 2 — Инвентаризация и контроль программных активов: помогает идентифицировать все программные активы и обеспечивает их актуальность с помощью последних исправлений безопасности.

3. Контроль 3 — Непрерывное управление уязвимостями: помогает в выявлении и устранении уязвимостей в программных и аппаратных активах.

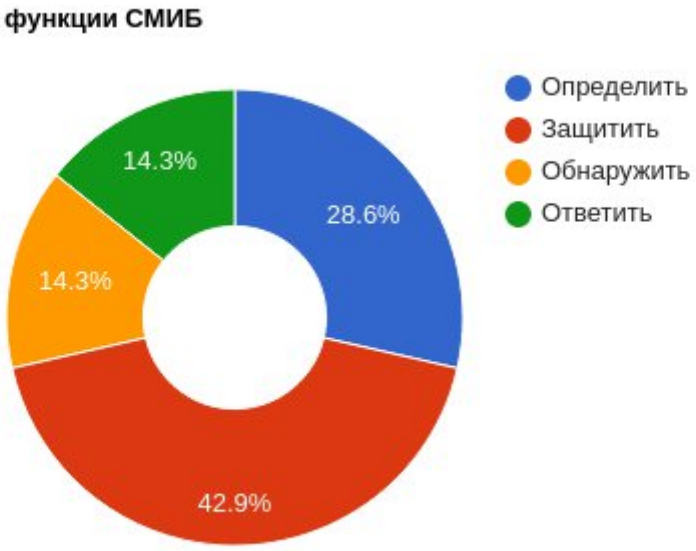
4. Элемент управления 5 — контролируемое использование административных привилегий: гарантирует, что административные привилегии предоставляются только уполномоченному персоналу и используются только в разрешенных целях.

5. Элемент управления 6 — Обслуживание, мониторинг и анализ журналов аудита. Помогает обнаруживать подозрительную активность и реагировать на нее путем анализа журналов аудита.

6. Control 7 — Защита электронной почты и веб-браузеров: помогает предотвратить фишинговые атаки через электронную почту и веб-браузеры.

7. Элемент управления 11 — Безопасная конфигурация сетевых устройств, таких как брандмауэры, маршрутизаторы и коммутаторы. Обеспечивает безопасную настройку сетевых устройств и регулярное обновление с использованием последних исправлений безопасности.

Чтобы определить, какие функции СМИБ необходимо улучшить в первую очередь для защиты от Carbank, можно создать граф, сопоставленных с каждой из пяти функций NIST CSF:



Из приведенной выше сводной таблицы видно, что в наибольшей доработке нуждается функция «Защита», за которой следует функция «Идентификация».

Поэтому для защиты от Carbank рекомендуется уделить первоочередное внимание реализации средств контроля, связанных с функциями защиты и идентификации NIST CSF.

Рассчитать окупаемость инвестиций (ROI) реализации средств контроля, связанных с функциями защиты и идентификации NIST CSF, для предотвращения атак Carbank.

Чтобы рассчитать окупаемость внедрения элементов управления, связанных с функциями защиты и идентификации NIST CSF, мы можем использовать следующую формулу:

ROI = (Чистая прибыль / Стоимость инвестиций) x 100

Где,

Чистая прибыль = общая экономия - стоимость инвестиций

Общая экономия = ожидаемый убыток до контроля - ожидаемый убыток после контроля

Ожидаемый убыток до контроля = потенциальный убыток x вероятность риска

Ожидаемый убыток после контроля = ожидаемый убыток до контроля - (ожидаемый убыток до контроля x снижение риска благодаря контролю)

Предположим, что потенциальный ущерб от атаки Carbank оценивается в 10 млн рублей, а вероятность атаки составляет 50%. Стоимость внедрения контроля, относящегося к функциям Защитить и Идентифицировать, составляет 2 млн рублей. Ожидаемое снижение риска благодаря средствам контроля оценивается в 70%.

Ожидаемый убыток до контроля = 10 000 000 x 0,5 = 5 000 000 руб.

Ожидаемый убыток после контроля = 5 000 000 - (5 000 000 x 0,7) = 1 500 000 руб.

Итого Сбережения = 5 000 000 - 1 500 000 = 3 500 000 рублей

Чистая прибыль = общая экономия - стоимость инвестиций = 3 500 000 - 2 000 000 = 1 500 000 руб.

ROI = (Чистая прибыль / Стоимость инвестиций) x 100 = (1 500 000 / 2 000 000) x 100 = 75%

Таким образом, окупаемость внедрения элементов управления, связанных с функциями защиты и идентификации NIST CSF, составляет 75%.