Business Email Compromise INVESTIGATION

BACKGROUND & SEQUENCE OF EVENTS

Корпоративная почта взломана и ее содержание изучено мошенниками

Спам фильтр компании изменен
Зарегистрирован фейковый домен
Первый email об изменении банковских реквизитов получен с фейкового адреса

MFA отключена
Первый трансфер на счет в Европе
Второй трансфер возвращен банком

Мошенники запросили еще одну замену реквизитов (банк другой Европейской страны)

Трансфер возвращен банком
Счет в первом банке закрыт
Третий запрос по изменению реквизитов

Мошенничество обнаружено

Апрель | Май | Июнь | Июль

KEY FINDINGS AND ISSUES

- Проверка на полиграфе оценивает участие сотрудников в мошенничестве как маловероятное
- На устройствах сотрудника не обнаружено никаких следов вредоносного ПО
- Доказательства предполагают, что роль сотрудника была важной предпосылкой для мошенничества, и некоторые из его заявлений противоречат другим задокументированным фактам.

- Есть явные доказательства того, что корпоративная электронная почта была взломана, и ее содержание было (и является) доступным для мошенников. Им удалось изменить настройки фильтра спама и использовать вложения из предыдущих писем, чтобы подделать учетные данные для этого мошенничества.

- В настройках защиты информации Клиента отсутствуют основные предпосылки для успешного расследования инцидентов, и конкретная конфигурация ИТ-инфраструктуры не позволяет получить цифровые доказательства для подтверждения основных версий расследования.

- Клиент подвергся вероятной атаке со стороны международной киберпреступной группы, которая последовательно проводит незаконные операции. Теперь у них есть информация из почтового ящика, и они будет продолжать использовать украденную информацию для других целей мошенничества против Клиента и / или его партнеров.

KEY FINDINGS AND ISSUES

- Корпоративные электронные письма других клиентов, вероятно, скомпрометированы и используются прямо сейчас или планируются к использованию в ближайшем будущем.

- В бизнес-процессах и структурах клиента отсутствуют эффективные механизмы, необходимые для обеспечения финансовой безопасности.

- Осведомленность сотрудников клиента о мерах по борьбе с мошенничеством и кибербезопасности недостаточна для предотвращения других видов мошенничества и возможной компрометации корпоративных ИТ-ресурсов в будущем.

ДАЛЬНЕЙШИЕ ВОЗМОЖНЫЕ ДЕЙСТВИЯ

Проверка на полиграфе сотрудников ИТ-отдела

Проверка их возможного участия
Обеспечение надежности персонала

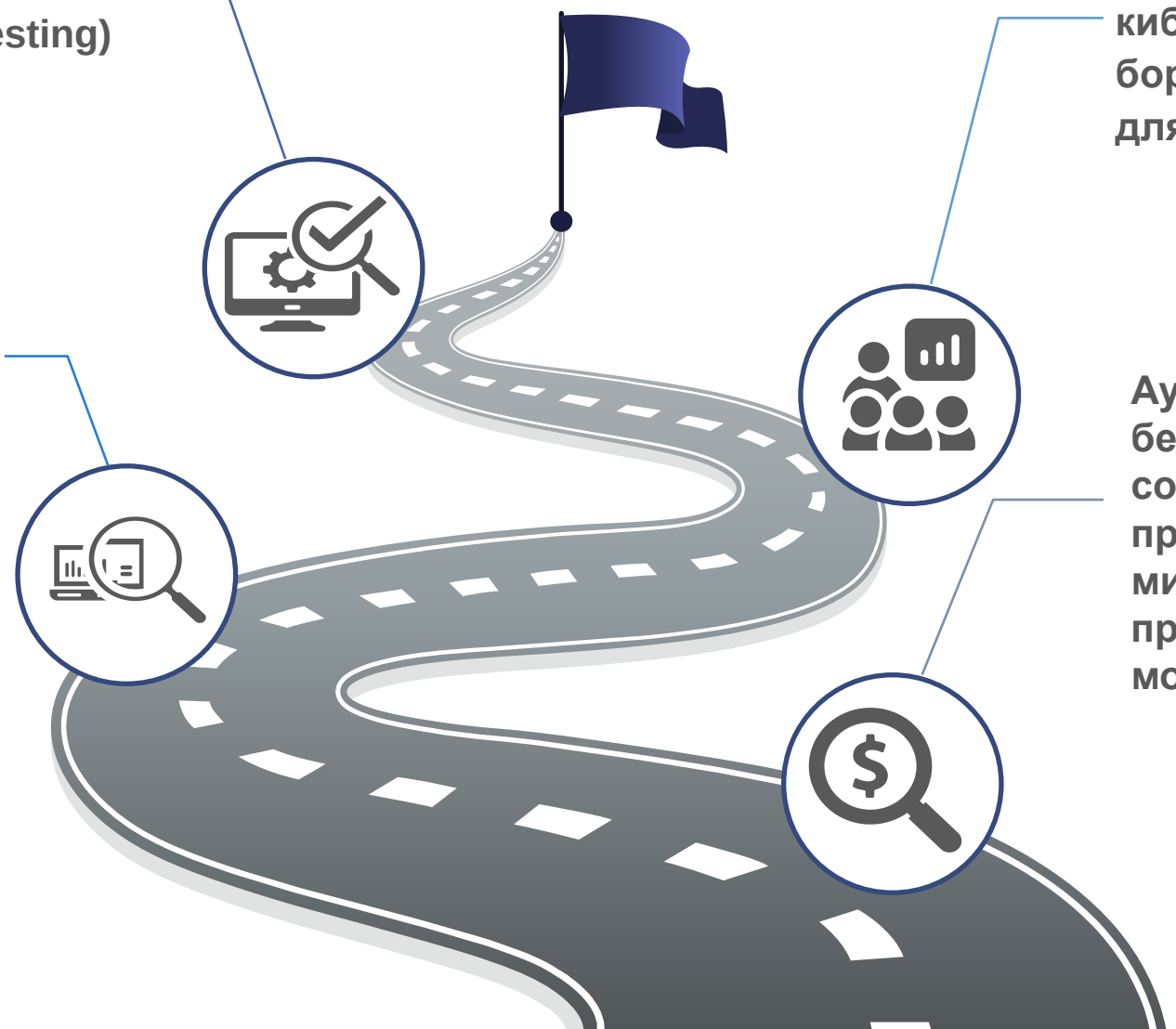
Уголовное расследование

Инициирование уголовного производства и его сопровождение

ДРУГИЕ РЕКОМЕНДУЕМЫЕ МЕРОПРИЯТИЯ

Тестирование на проникновение (Penetration testing)

Аудит кибербезопасности и согласование ИТ-стратегии



Тренинг по кибербезопасности и борьбе с мошенничеством для сотрудников клиента

Аудит финансовой безопасности и согласование бизнес-процессов с целью минимизации рисков и предотвращения мошенничества в будущем