Ассоциация участников МастерКард

20.11.2013

Развитие современных платежных инструментов и банковских приложений как элемент устойчивого и эффективного функционирования НПС России

АРБ. Москва. Инфопространство

Учёт рисков мошенничества с ЭСП, как необходимое условие успешного внедрения новых банковских продуктов и технологий.

Социальная инженерия (на примере банкоматов).

Ассоциация участников МастерКард

Основные угрозы

- **Скимминг** (skimming)– кража с использованием специальных технических средств данных, записанных на магнитную полосу карты, а также ПИН-кода, с целью дальнейшего изготовления поддельных карт и, как правило, последующего несанкционированного снятия наличных средств
- **Захват наличных (**cash trapping) - использование мошеннических средств и способов для физического захвата наличных денежных средств клиента, при совершении им лигитимной операции в банкомате
- **Захват карты (**card trapping) – использование мошеннических средств и способов для физического захвата карты клиента и выведывания ПИН-кода, с целью последующего снятия денег с этой карты в банкомате
- **Взломы/ограбления/взрывы/кража банкоматов (**Ram Raids/ATM burglary/ Robbery/Explosion) – преступное посягательство на наличные средства, находящиеся в сейфе банкомата с использованием различных способов физического и технического воздействия
- **Вредоносное программное обеспечение (**ATM malware) – использование специально написанных и внедрённых в компьютер банкомата «вирусов», с целью кражи информации по карте и ПИН-кода либо напрямую наличных средств, находящихся в банкомате
- **Transaction Reversal Fraud (**TRF) – мошенничество, связанное с получением наличных денежных средств и одновременным негативным воздействием на работу банкомата, а также процессингового центра (хоста), которое не позволяет корректно завершить операцию по выдаче денег, в результате чего баланс по карте не меняется (манипулирование карточным счётом)
- **Поддельные банкоматы** (Fake ATMs) - кража с использованием поддельных АТМ данных по карте, а также ПИН-кода
- **Социальная инженерия (**social engineering) – мошенническое воздействие на сознание держателя карты с целью принудить его к совершению платёжной операции либо к переводу денег с помощью банкомата

Ассоциация участников МастерКард

Предпосылки

- **Новые нехарактерные для банкомата функции** – в настоящее время это многофункциональное устройство для оказания дистанционных банковских услуг: выдача наличных; платежи за услуги сторонних организаций; денежные переводы; пополнение электронных кошельков и другое
- **Относительно сложный интерфейс взаимодействия**
- **Относительно слабая информированность об угрозах**

Ассоциация участников МастерКард

Классификация социальной инженерии, как угрозы

- **Телефонное мошенничество**

– звонок держателю карты;

- звонки в call-center (**vishing**)

- **Интернет мошенничество, цифровые устройства (digit):**

- Phishing – массовая рассылка электронных писем с целью: прямой ответ на запрос; активация вложений и заражение вредоносным ПО; отсылка на сайты с последующим выведыванием критически важных данных; и др.
- Spear phishing – целенаправленная рассылка писем;
- Smishing – СМС рассылка
- **Вредоносное ПО (Malware, “out of scope”) на хосте**

Ассоциация участников МастерКард

Целевая аудитория для атаки

- **Массовый сегмент/физические лица/держатели карт (Retail Consumers)**

- **Организации/банки/Процессинги (Commercial Customers)**

Ассоциация участников МастерКард

Меры противодействия

- **Информирование/Уведомление и Обучение (Awareness & Education)**
- **Предотвращение и Мониторинг (Prevention & Monitoring)**
- **Сотрудничество и Взаимодействие (Collaboration & Cooperation)**

Ассоциация участников МастерКард

Информирование/Уведомление и Обучение

- **Разделение и учёт специфики внутренней (сотрудники компаний) и внешней (держатели карт) социальной инженерии**
- **Повышенное внимание к этой угрозе со стороны сотрудников банка/организаций**
- **Тестирование сотрудников**
- **Организация информационно-пропагандистких компаний среди клиентов/населения**
- **Доведение до сведения клиентов информации о том, какие вопросы могут быть заданы со стороны банков, а какие нет (например, ПИН-код)**
- **Создание комфортных условий для связи клиента с банком в ситуации, когда он/она стали жертвой (чувство вины и глупости)**

Ассоциация участников МастерКард

Предотвращение и Мониторинг

- **Использование в стратегии предотвращения маркетинговых инструментов и возможностей банка**
- **При контакте с клиентом использовать адекватную и понятную для клиента тактику диалога**
- **Использование динамической двухфакторной идентификации кдиента**
- **Использоване других достоверных способов идентификации**
- **Мониторинг неактивных счётов (например, более 6 месяцев)**
- **Перепроверка/уведомление изменений в данных клиента**
- **Маскирование данныхъ на странице банка**
- **Создание профиля клиента**
- **Проактивный монитори нг социальных сетей**
- **Создание системы поиска и мониторинга сайтов кардеров**
- **Создание многоуровневой, построенной на разных правилах внутренней системы противодействия и защиты**
- **Взавимодействие различных департаментов и контроль**

Ассоциация участников МастерКард

Сотрудничество и Взаимодействие

- **Важно знать соответствующее подразделерние в правоохранительных органах, которое может быть привлечено к расследованию инцидентов, связанных с социальной инженерией, как при атаке на банк, так и угрозах в адрес клиентов**
- **Важно иметь прямой контакт с МВД и знать, какая им требуется информация в этом случае**
- **Целесообразно прописать и закрепить регламенты взаимодействия при такого рода атаках**
- **Определить в банке ответвтенное лицо за взаимодействие как с подразделениями внутри организации, так и с МВД**
- **Подготовить максимально полную информацию для расследования**
- **Раъяснение роли и места всех сторон-участников процесса**
- **МЕЖБАНКОВСКОЕ ВЗАИМОДЕЙСТВИЕ!!!**

Благодарю за внимание!