ЗАТРАТЫ НА АНТИФРОД. КАК СОБЛЮСТИ БАЛАНС МЕЖДУ РАСХОДАМИ И ПОТЕРЯМИ?

Шмелев Александр, руководитель направления консалтинга
по информационной безопасности AKTIV.CONSULTING

ПРОВЕРЕНО. ФРОДА НЕТ.

AKTIV.
CONSULTING

Одной из важных тем при обсуждении вопросов обеспечения ИБ с клиентами AKTIV.CONSULTING является тема разумного баланса между затратами на антифрод системы и возможными потерями от различного рода мошенничества. Существует ли золотая середина? Давайте попробуем разобраться.

АНТИФРОД В ОРГАНИЗАЦИИ.
ВМЕСТЕ ИЛИ ПОРОЗНЬ?

Очень часто в финансовых организациях работа с внешним мошенничеством ведется сразу несколькими подразделениями: отдел обслуживания физлиц, юрлиц, ДБО, пластиковые карты и т.д.). Что же касается внутренних угроз мошенничества, операций в отсутствие клиента, введения в заблуждение и т.д.- этой проблемой в финансовой организации зачастую вообще никто не занимается. Подобная ситуация приводит к целому ряду сложностей и проблем.

Одна из них - отсутствие кроссканальности и сквозного процесса антифрода, когда невозможно объединить и проанализировать данные об угрозах мошенничества по различным направлениям: например, ДБО или банкоматному обслуживанию. В результате мы имеем неточность в настройке антифрода, «бьем из пушки по воробьям» и получаем низкую результативность. Более того, у финансовой организации в данном случае нет возможности оперативно среагировать на инцидент.

Весьма примечательным кейсом такой “антифрод-разобщенности” может служить ситуация, когда сотрудники офиса обслуживания подменили номера телефонов владельцев «спящих» счетов и завладели их денежными средствами. Результатом этих мошеннических действий стали потери для банка в размере 10 млн.рублей плюс негативные последствия для репутации банка, а также дополнительные расходы и ограничения на основании требований Положения 716-П. А ведь инцидента могло бы и не произойти, если бы в антифрод систему попадала информация о действиях сотрудников "фронта", которую можно было бы сопоставить с имеющейся информацией по движениям средств по счетам и картам клиентов.

AKTIV.
CONSULTING

ТАК КАК ЖЕ РЕШИТЬ ПРОБЛЕМУ?

В идеале необходимо объединить работу по предотвращению мошенничества и сбор соответствующих данных «под одну крышу», в одно подразделение, отвечающее за все направления антифрода.

В частности, это поможет оптимизировать суммарные расходы на антифрод. Если брать некий гипотетический банк с усредненными показателями в 2 млн. карт, 1 млн. активных пользователей, 150-200 тыс. операций в день, средний чек на операцию 1-2 тыс. рублей, затраты на обслуживание его антифрод системы составят сегодня 2-3 млн. рублей на одно из трех направлений антифрода. Суммарно это составит 7-8 млн. рублей в год.

Если же установить единую для банка антифрод систему, затраты на ее обслуживание в последующие года обойдется в 9-10 млн ежегодно. Несмотря на имеющуюся разницу в стоимости обслуживания и на необходимые затраты на внедрение единой системы, ее эффективность значительно выше за счет возможности объединения потоков данных.

Например, в рамках описанного выше кейса, единая система антифрода позволила бы избежать потерь, соразмерных с ее стоимостью. Также не стоит забывать про необходимость резервирования средств в соответствии с требованиями Положения 716-П.

AKTIV.
CONSULTING

МОГУТ ЛИ МАЛЫЕ ВЛОЖЕНИЯ ПРЕДОТВРАТИТЬ МИЛЛИОННЫЕ ПОТЕРИ?

Зачастую небольшие доработки информационных систем банка помогают избежать потери в результате мошенничества. Но, к сожалению, не всегда удается донести ценность этих доработок до менеджмента. А ведь затраты на них не соизмеримы с возможными потерями!

Опять обратимся к кейсу. В результате инфраструктурной атаки или социнженерии мошенники получили доступ к личным кабинетам около 100 клиентов. При этом они использовали 10 мобильных устройств для вывода средств со счетов этих клиентов. Изначально в банке планировали реализовать привязку каждого клиента к устройству, с которого осуществляется вход в личные кабинеты, т.е. контролировать уникальность каждого из них. Данная доработка оценивалась в сумму 300-500 тыс. рублей. Однако описанные доработки так и не были внедрены.

В результате мошеннический действий по этому кейсу банк потерял 7 млн. рублей. И тут ключевая проблема заключалась как раз в отсутствии взаимопонимания между ИБ, ИТ и бизнесом. Одни не смогли аргументировать, другие не захотели услышать. К сожалению, это довольно распространённая ситуация, в которой можно посоветовать коллегам из ИБ проявлять больше инициативы и укреплять аргументы с помощью понятных бизнесу метрик.

И в завершении статьи хочется резюмировать: собирайте и используйте более полные данные и расширяйте число каналов сбора этих данных. Это поможет в борьбе с мошенничеством, в частности, с социнженерией, и позволит избежать финансовых и репутационных потерь, а также регуляторных рисков.