Андрей БАЖИН,

руководитель Департамента информационной безопасности, банк «УРАЛСИБ»

Принципы построения системы защиты от несанкционированного доступа к финансовым услугам

В статье рассмотрены обстоятельства, которые создают возможности мошенничества в сфере ИТ, стратегические решения по созданию системы противодействия мошенничеству и общие принципы построения такой системы.

Несанкционированный доступ к финансовым услугам банков направлен, главным образом, на карточные продукты и системы дистанционного банковского обслуживания (ДБО). И это понятно: деньги сразу можно использовать или быстро перевести в иные активы. Переходя к цифрам, приведем информацию, полученную от Group-IB: «По данным МВД (УСТМ), в г. Москве каждые два месяца регистрируется шесть случаев мошенничеств с использованием систем ДБО. Средний ущерб по каждому из инцидентов составляет 3-5 млн. рублей. Это данные по зарегистрированным заявлениям.

Реальных инцидентов в десятки раз больше».

Возможности несанкционированного доступа к финансовым услугам

Можно назвать три основные возможности несанкционированного доступа к системам ДБО, на которые достаточно просто повлиять, изменив внутренние процессы.

Первая возможность имеет самое непосредственное отношение к сфере высоких технологий – это уязвимости в системах и недостаточные средства защиты.

Вторая связана с использованием сотрудниками своих служебных полномочий в личных целях. Третья – с отсутствием контроля за типовыми рисками (как в области технологий, так и в области процессов, являющихся частью программы по управлению фродом).

Чтобы исключить факты несанкционированного доступа к финансовым услугам, необходимо разработать и внедрить программу по противодействию мошенничеству. Если такой программы нет или если у такой программы нет спонсорской поддержки, успех маловероятен. Именно системный подход закладывает механизмы, минимизирующие возможности совершения финансовых преступлений.

Но возможности – это только открытая дверь, чтобы ею воспользоваться, нужна мотивация, которая имеет свои всплески и спады. Отдельно отметим, что во время кризиса количество преступлений, как правило, возрастает.

Продолжая рассматривать обстоятельства, которые благоприятствуют финансовым мошенничествам с помощью информационных технологий, отдельно остановимся на возможности уйти от ответственности. Доказать в суде факт несанкционированного доступа достаточно сложно, особенно в случае, если он совершен из-за рубежа. Однако в последнее время в этом направлении наметились позитивные сдвиги: внедряется такие стандарты, как PCI DSS, PA DSS, а в статью 187 УК РФ внесены изменения, касающееся карточного фрода.

Но, пожалуй, наиболее критичное обстоятельство, благоприятствующее несанкционированному доступу – это незнание и (или нежелание) пользователей финансовых услуг знать и применять элементарные правила безопасности. Так пользователи ДБО зачастую не устанавливают на свои компьютеры постоянно обновляемое лицензионное антивирусное программное обеспечение, а владельцы карточек хранят и карточку, и пин-код в одном кошельке или записывают пин-код в телефон.

Социальная инженерия

При совершении преступлений в сфере высоких технологий могут использоваться и методы социальной инженерии. Так, доверчивых людей могут обмануть и предложить открыть карточный счет в банке для «доброго» друга, у которого нет паспорта и которому нужно получить деньги от родителей. Потом окажется, что через эту карточку были обналичены денежные средства, «доброго» друга и след простыл, зато у владельца карточки появятся проблемы.

Стратегия противодействия мошенничеству в сфере ИТ

Ополчением войну не выиграть, и для противодействия мошенничеству должны быть приняты стратегические решения. При принятии этих решений должна учитываться отраслевая статистика и основные факторы риска фрода, присущие конкретной компании.

Прежде всего, необходимо концептуальное понимание ролей основных служб, которые отвечают за конечный результат. Обязательно должно быть налажено взаимодействие служб информационной безопасности, внутренней безопасности, операционной поддержки, процессинга, AML (службы противодействия легализации доходов, полученных преступным путем) и, возможно, служб PR и GR (службы взаимодействия компании с органами власти). После того как будут концептуально распределены зоны ответственности перечисленных служб, требуется детализация всех соответствующих регламентов и процедур. Распределение зон ответственности ни в коем случае не должно быть формальным – это должен быть реально работающий механизм, нацеленный на снижение рисков. Кроме того, должны быть определены критерии принятия решений.

На этом этапе закладывается организационная и методологическая база противодействия

мошенничеству, формируется перечень контрольных мероприятий нацеленных на
а) профилактику
б) выявление
в) реагирование на инциденты, связанные с несанкционированным доступом.

Следующий шаг – детализация концепции и создание программы мер по противодействию фроду, определение бюджета, реализация мероприятий по техническому и организационному обеспечению, финальная настройка контрольной среды.
Для достижения успеха, во-первых, программа должна содержать критерии эффективности мероприятий, разработанных для предотвращения мошенничества, а во-вторых, необходим достаточный уровень зрелости системы корпоративного управления, ИТ, службы внутренней безопасности. В противном случае речь о системном противодействии мошенничеству идти не может – только о мерах противодействия наиболее значимым типовым рискам.
В завершающей стадии процесс должен быть отработан на инциденте, который бы прошел все основные стадии, в том числе, возбуждение уголовного дела.

Общие принципы построения процесса противодействия мошенничеству

Прежде всего, надо четко определиться, будет ли противодействие мошенничеству организовано как единый процесс или же это будет несколько независимых процессов. Например, будет назначен всего один ответственный, курирующий случаи несанкционированного доступа по всем транзакционным каналам (карточки, ДБО, банковские системы и т.д.) или же ответственных будет несколько.
Если процесс будет централизованным, то целесообразно учитывать его взаимосвязь с общекорпоративным процессом управления рисками и процессами внутреннего контроля.
Если же централизованную систему противодействию мошенничеству внедрить сразу сложно или даже невозможно, то нужно

четко понять, какие именно элементы децентрализованной системы противодействия мошенничеству будут внедряться. Вместе эти элементы должны образовать своего рода структурный зонтик, охватывающий все выделенные риски.

После того, как определены функции, на которые распадается система противодействия мошенничеству, и они распределены между исполнителями, встает вопрос технологий защиты, потому что без них проблему не решить.

Технологии защиты

Для обеспечения защиты от несанкционированного доступа нужны как классические средства обеспечения защиты информационных систем (антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений, средства шифрования и криптографии, одноразовые пароли на транзакции и т.д.), так и специализированные системы, позволяющие выявлять несанкционированный доступ на самых ранних стадиях. Последние подразделяются на три вида:

А. FMS (Fraud Management System) – это системы, которые в целом охватывают основные электронные каналы. Они позволяют применить более-менее типовые правила для того, чтобы выявлять те или иные схемы мошенничества. Как правило, эти системы работают с информацией на уровне бизнес-логики, то есть не просто с каким-то платежом, а с целым рядом показателей, которые обрабатываются статистическими методами. Количество ложных срабатываний у таких систем при правильной настройке достаточно низкое.

Б. SIEM (Security Information and Event Management) – это системы, предназначенные для первичной фильтрации и выявления системных событий на уровне электронных журналов. Используются в основном в ИБ и ИТ для мониторинга и корреляции событий в сетевой и прикладной инфраструктуре. Эти системы не в состоянии с высокой степенью точности отличить фрод от не фрода, но позволяют проводить первичную обработку данных, фильтрация и корреляцию.

Следует отметить, что западные FMS и SIEM-системы практически не учитывают отечественную специфику. Наверное, именно поэтому сейчас наметилась тенденция внедрения российских разработок.

В. Системы электронного архива (например, архив электронной почты). Они необходимы для установления всех деталей инцидента.

При проектировании архитектуры решений необходимо уделять

большое внимание возможности получения требуемых данных и оценке необходимого времени для написания коннекторов. Иначе может получиться, так, что после внедрения дорогой FMS-системы сотрудники компании не смогут наполнить ее требуемыми для анализа данными. При создании процесса противодействия мошенничеству очень важно понимать, что после того, как инцидент произошел, должна быть обеспечена возможность сбора юридически доказательной базы. Если процедуры сбора юридически значимой доказательной базы нет и отсутствует опыт взаимодействия с МВД, то в ряде случаев расследование инцидента может быть существенно затруднено.

В заключении хочу отметить, что противодействие мошенничеству – это сложная задача, которая требует системного подхода. Интеграторов и консультантов, которые могли бы поставить процесс противодействия мошенничеству «от и до» найти сложно, т.к. область достаточно новая, и находится она на стыке ИБ, ИТ, юриспруденции, бизнес-логики и оперативно-розыскных мероприятий. Но вопрос требует решения и лучше раньше начинать выстраивать процесс по управлению фродом, чем потом бороться с его последствиями.