hēlios
INFORMATION TECHNOLOGIES

Комплексный подход к обнаружению мошеннических действий в платёжных системах

Волков Олег

14 февраля 2013 г.

Что есть платёжная система

Платёжная система - это совокупность правил, договорных отношений, технологий, методик расчёта, внутренних и внешних нормативных актов, которые позволяют всем участникам производить финансовые операции и расчёты друг с другом.

Эффективность платёжной системы - это своевременность и надёжность передачи и учёта платёжных ресурсов, выделяемых на проведение платежей.

Инструменты автоматизации

Системы учёта депозитов

Карточные системы

Системы денежных переводов

Системы ДБО

Системы учёта займов

Системы РКО

Ущерб от мошеннических действий

В России за 2012 год ущерб от действий киберпреступников составил порядка $2 млрд.

(Symantec: «Norton Cybercrime Report 2012»)

Самая большая сумма мошеннической транзакции, попытка проведения которой была предпринята в банковской системе РФ в 2012 году = 400 млн. рублей.

(«конференция Antifraud 2012»)

Мошеннический действия со стороны внешних злоумышленников

- Кража денежных средств с банковских карт:
  - ✓ Кардинг
  - ✓ Скимминг
  - ✓ Фишинг
- Кража средств в системах ДБО:
  - ✓ Подмена реквизитов платежа в сессии
  - ✓ Кража ключей ЭЦП
  - ✓ Получение доступа к АРМ оператора ДБО
- Кража средств при платежах в Интернете:
  - ✓ Взлом учётной записи
  - ✓ Фишинг

Мошеннические действия со стороны инсайдеров

- ✓ хищения с использованием мемориальных ордеров
- ✓ вступления в сговор с клиентом банка, путём увеличения остатка его личного счета с последующим разделением полученных средств
- ✓ составления подложных документов, отражающих проведение клиринговых операций (взаимозачёт встречных требований).
- ✓ перевод денежных средств на собственные лицевые счета
- ✓ округление сумм, находящихся на счетах клиентов банка
- ✓ инсценировка «арифметических ошибок», «неправильного исчисления процентов»
- ✓ обналичивание средств за определённое вознаграждение»
- ✓ выдача крупных кредитов (превышающих 5 процентов капитала банка) без уведомления членов правления либо членов кредитного комитета банка
- ✓ выдача необеспеченных залогом кредитов
- ✓ занижения дохода, полученного в форме ссудных процентов

Тенденции мошеннических действий

Динамика мошеннических действий постоянно меняется от снижения к увеличению и обратно

- Злоумышленники становятся более опытными
- Атаки становятся всё более изощренными

Факторы успеха в борьбе с мошенничеством

- Мониторинг активности внешних и внутренних пользователей
- Управление правами доступа пользователей (принцип «минимально необходимого набора прав»)
- Усиленный контроль за наиболее критичными операциями (принцип «четырёх глаз»)
- Контроль привилегированных учётных записей (контроль администраторов)
- Профилактика фишинга (программы по информированию пользователей)
- Тщательный скрининг новых сотрудников

Требования к инструментам мониторинга мошеннических действий

- Минимальное воздействие на производительность информационных систем
- Возможность записи и воспроизведений сессий пользователей
- Профилирование пользователей и скорринг
- Поддержка различных источников данных
- Возможность остановки транзакции до принятия решения
- Эргономичность центров расследования инцидентов
- Детализация и визуализация отчётов
- Гибкость и эргономика настройки правил
- Универсальность использования антифрод-системы

hēlios
INFORMATION TECHNOLOGIES

Спасибо за внимание?