Посилання на статтю

Пилипенко А.И. Классификация угроз информационной безопасности в проектах нематериальной сферы (на примере индустрии платежных карт) / А.И. Пилипенко, С.В. Пилипенко // Управление проектами и развитие производства: Сб.науч.раб. - М.: изд-во ВНУ им. Даля, 2008. - № 3 (27). - С. 121-129. - Режим доступу: http://www.pmdp.org.ua/images/Journal/27/08paiipk.pdf

УДК 005+004:336.71

А.И. Пилипенко, С.В. Пилипенко

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЕКТАХ НЕМАТЕРИАЛЬНОЙ СФЕРЫ (НА ПРИМЕРЕ ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ)

Предложена классификация угроз информационной безопасности, позволяющая выявлять и анализировать риски в индустрии платежных карт, а также определять направления, на которых целесообразно концентрировать основные ресурсы в проектах информационной безопасности нематериальной сферы. Рис. 3, ист. 5.

Ключевые слова: угроза, риск, информационная безопасность, платежная система.

А.І.Пилипенко, С.В. Пилипенко

КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЕКТАХ НЕМАТЕРІАЛЬНОЇ СФЕРИ (НА ПРИКЛАДІ ІНДУСТРІЇ ПЛАТІЖНИХ КАРТ)

Запропоновано класифікацію загроз інформаційної безпеки, яка дозволяє виявляти і аналізувати ризики в індустрії платіжних карт, а також визначати напрями, на яких доцільно концентрувати основні ресурси в проектах інформаційної безпеки нематеріальної сфери. Рис. 3, дж. 5.

Ключові слова: загроза, ризик, інформаційна безпека, платіжна система.

A.I.Pilipenko, S.V.Pilipenko

INFORMATION SAFETY THREATS CLASSIFICATION IN NON-MATERIAL FIELD PROJECTS (ON THE EXAMPLE OF PAYMENT CARDS INDUSTRY

Information safety threats classification is offered, which allows defining and analysing payment cards industry risks. Besides, it allows knowing directions for concentration main resourses in information safety projects in non-material field.

Keywords: danger, risk, information security, the payment system.

Постановка проблемы. Согласно закону Украины [1], *информационная безопасность* – состояние защищенности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесение вреда через: неполноту, несвоевременность и недостоверность используемой информации; негативное информационное влияние; негативные последствия

применения информационных технологий; несанкционированное распространение, использование и *нарушение целостности, конфиденциальности и доступности информации*. Управление рисками, включая анализ возможных угроз, относится к административному уровню информационной безопасности, поскольку только руководство организации может выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Нематериальная сфера непосредственно не создает материальные блага, но обеспечивает разнообразные потребности людей, бытовые и духовные, здравоохранения и образования, другие услуги. К этой сфере также относится индустрия платежных карт. По данным Украинской межбанковской ассоциации членов платежных систем «ЕМА» на 1 октября 2008 года украинские банки выпустили 63 577 тыс. пластиковых карт платежных систем Visa и MasterCard, что на 1 600 тыс. карт більше, чем на 1 сентября [2]. По мере увеличения объемов эмитируемых карт значительно увеличились и убытки банков от мошеннических действий по операциям с платежными картами. В связи с этим предотвращение угроз информационной безопасности в индустрии платежных карт является актуальной проблемой.

Анализ последних исследований и публикаций. Управление рисками, равно как и выработка собственной политики безопасности в нематериальной сфере, особо нужны для тех организаций, информационные системы которых и/или обрабатываемые данные являются частью платежной системы. Риск существует тогда, когда лицо, принимающее решение, не знает заранее его результатов, но способно установить вероятные угрозы, объективное распределение вероятностей возможных состояний внешней среды и связанных с ними последствий или результатов [3].

Выделение не решенных ранее частей общей проблемы. В публикациях, посвященных исследованию рисков в карточном бизнесе, отсутствует классификация угроз информационной безопасности с точки зрения теории принятия управленческого решения. Такая классификация необходима для дальнейшего развития методологии управления рисками в проектах информационной безопасности в нематериальной сфере.

Целью данной статьи является разработка классификации угроз информационной безопасности в индустрии платежных карт, позволяющей выявлять и анализировать риски в проектах информационной безопасности в нематериальной сфере.

Основной материал исследования. Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность. Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, – злоумышленником. Потенциальные злоумышленники называются источниками угрозы [4].

В индустрии платежных карт угроза чаще всего возникает из-за уязвимостей в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать уязвимость, и до того, когда она ликвидируется, называется окном опасности, ассоциированным с данной уязвимостью. Пока существует окно опасности, возможны успешные атаки на информационную систему [4].

Не все угрозы являются следствием ошибок или просчетов; они существуют в силу самой природы современных информационных систем. Например, угроза отключения электричества или выхода его параметров за допустимые границы

происходит по причине зависимости аппаратного обеспечения информационных систем от электропитания.

Понятие «угроза» в разных ситуациях трактуется по-разному. Например, для подчеркнуто открытой организации может просто не существовать угроз конфиденциальности, так как вся информация считается общедоступной. И все же в большинстве случаев нелегальный доступ считается серьезной опасностью.

Рассмотрим отношение к угрозам с точки зрения банка в карточном бизнесе. Их можно классифицировать по нескольким критериям:

– аспект информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

– компонент информационных систем, на который угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

– способ осуществления угроз (случайные/преднамеренные действия природного/техногенного характера);

– расположение источника угроз (внутри/вне рассматриваемой информационной системы).

Наиболее распространенные угрозы доступности. Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются непосредственными угрозами (неправильно введенные данные или ошибка в программе, вызвавшие крах системы), иногда они создают уязвимости, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования).

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – это максимальная автоматизация и строгий контроль над правильностью совершаемых действий.

Другие угрозы доступности классифицируем по компонентам информационных систем, на которые нацелены угрозы:

– отказ пользователей (нежелание работать с информационной системой; невозможность работать с системой, так как нет соответствующей подготовки; невозможность работать с системой из-за отсутствия технической поддержки);

– внутренний отказ информационной системы (отступление от установленных правил эксплуатации; выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала; ошибки при (пере)конфигурировании системы; отказы программного и аппаратного обеспечения; разрушение данных; разрушение или повреждение аппаратуры);

– отказ поддерживающей инфраструктуры.

Особую угрозу доступности для информационной безопасности банка-эмитента в карточном бизнесе представляет мошенничество в среде Internet. Схема взаимодействия мошенников следующая:

– мошенники одной группировки не знают друг друга;

– общение с использованием чатов, выдуманных псевдонимов;

– взаимодействие на международном уровне;

– безопасность для группировки в случае поимки одного из участников.

К угрозам банка-эквайера относится мошенничество торгового предприятия:

– обслуживание недействительных/поддельных карточек;

– ручной ввод реквизитов карточки;

– мошеннические действия персонала торговой точки;

– кража реквизитов действующих карточек с целью их дальнейшей подделки;

– создание торговой точки с целью мошенничества;

– электронная коммерция.

Основные угрозы целостности. На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) располагаются кражи и подлоги. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Целесообразно провести различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (являющийся, как правило, штатным сотрудником) может:

– ввести неверные данные;

– изменить данные.

Существует опасность слепо доверять компьютерную информацию. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя. Отметим, что последняя угроза актуальна даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить безотказность, то компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы по отношению к нарушению целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного программного обеспечения – пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

К угрозам целостности безопасности банка-эмитента относятся:

– технические сбои;

– халатность персонала;

– ошибки в проведении рекламационной работы/несвоевременное опротестование транзакций;

– изменение курсов валют;

– комиссии банка;

– потеря информации;

– неверная идентификация клиента;

– повторная/несвоевременная обработка транзакций.

К угрозам целостности безопасности банка-эквайера относятся следующие операции:

– повторная обработка операций;

– позднее выставление операций к оплате;

– утеря документов;

– сбои в работе оборудования.

Тенденции в сфере мошенничества в банкоматной сети, которые приводят к нарушению целостности информационной безопасности, такие:

– перехват авторизационных запросов с подстановкой авторизационных ответов;

– различные способы подключения и дислокации банкоматов (хольные/уличные, в людных/безлюдных местах).

Основные угрозы конфиденциальности. Конфиденциальную информацию можно разделить на два класса – предметную и служебную. Служебная информация (такая, например, как пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато несанкционированным доступом ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Описанный класс уязвимостей можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Угроза состоит в доступности информации (паролей). В этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает вполне возможной реализацию угрозы перехвата данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея тут одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании информационной системы, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются выставки, на которые многие организации отправляют оборудование из производственной сети, со всеми хранящимися на этих носителях данными. Остаются прежними пароли, при удаленном доступе они по-прежнему передаются в открытом виде.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, установить их, например, на кабельную сеть может даже уборщица, так что эту угрозу нужно принимать во внимание не только по отношению к внешним, но и к внутренним коммуникациям.

Опасной нетехнической угрозой конфиденциальности являются методы морально психологического воздействия, такие как «маскарад» – выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д.

Угрозу конфиденциальности для информационной безопасности банка представляет фишинг (Phishing) – получение информации о параметрах карты через фальшивые сайты. В США на протяжении 2006-2007 года было зафиксировано 84 млн посланий. На 21% посланий ответили клиенты, вследствие чего убытки составили 1,8 млрд $ USD. Пример фишинга в Украине представлен на рис. 1.

Существуют такие разновидности фишинга:

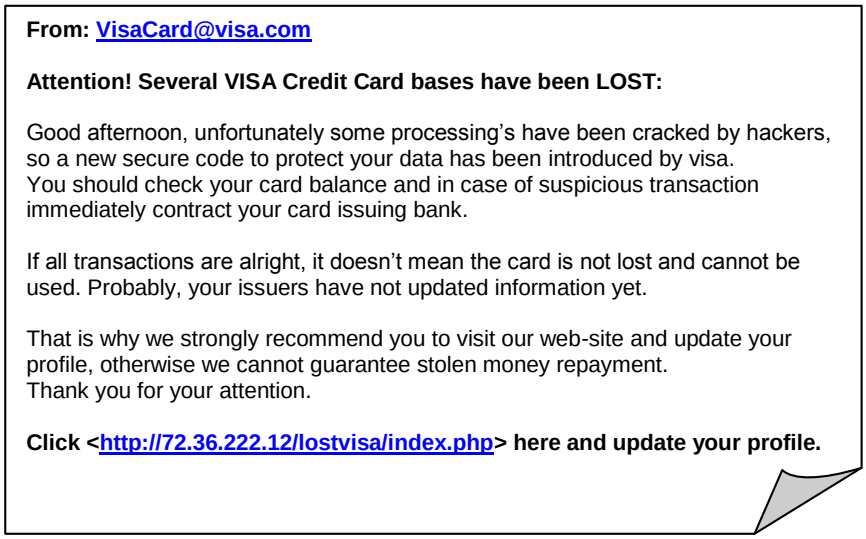
– вишинг – кража данных посредством телефона, используя автодозвон, с целью получения информации по карте;

– фарминг – создание мошеннических сайтов и смена IP адресов таким образом, чтобы перенаправить держателя на мошеннический сайт.

Мошенничество со стороны держателей карточек относится к рискам банка-эквайера:

– использование поддельных карточек;
– использование недействительных карточек;
– использование утерянных/украденных платежных карточек;
– злоупотребление подлимитными операциями.

Копирование магнитной полосы/PIN-кода при помощи устройств, несанкционированно установленных мошенниками в POS-терминалах также составляет угрозу конфиденциальности.


From: VisaCard@visa.com

Attention! Several VISA Credit Card bases have been LOST:

Good afternoon, unfortunately some processing's have been cracked by hackers, so a new secure code to protect your data has been introduced by visa.
You should check your card balance and in case of suspicious transaction immediately contract your card issuing bank.

If all transactions are alright, it doesn't mean the card is not lost and cannot be used. Probably, your issuers have not updated information yet.

That is why we strongly recommend you to visit our web-site and update your profile, otherwise we cannot guarantee stolen money repayment.
Thank you for your attention.

Click <http://72.36.222.12/lostvisa/index.php> here and update your profile.

Рис. 1. Пример фишинга в Украине

Угрозы в банкоматной сети составляют:

– потенциальная возможность доступа к PIN-клавиатуре, кард-ридеру банкомата;
– кража данных в банкоматах, подключенных через радиосети;
– компрометация данных путем скимминга и фишинга и использование карт в банкомате;
– использование накладных скиммингових устройств;
– использование видеокамер, накладок на клавиатуру;
– кража информации (фишинг, радиосети).

Вредоносное программное обеспечение. Одним из опаснейших видов атак является внедрение в атакуемые системы вредоносного программного обеспечения (ПО).

Существуют следующие грани вредоносного ПО:

– вредоносная функция;
– способ распространения;
– внешнее представление.

Спектр вредоносных функций неограничен, поскольку она, как и любая другая программа, может характеризоваться сколь угодно сложной логикой, но обычно вредоносные функции предназначаются для:

– внедрения другого вредоносного ПО;

– получения контроля над атакуемой системой;
– агрессивного потребления ресурсов;
– изменения или разрушения программ и/или данных.

По механизму распространения различают:

– вирусы – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

– «черви» – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по информационной системе и их выполнение (для активизации вируса требуется запуск зараженной программы).

Обычно вирусы распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на сетевые «путешествия».

Несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил компьютерной гигиены сводит риск заражения практически к нулю. Там где работают, а не играют, число зараженных компьютеров составляет лишь доли процента.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье – так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов – Java-аплеты, загружаемые на пользовательский компьютер и интерпретируемые Интернет-навигаторами.

В индустрии платежных карт угрозу для информационной безопасности представляет скимминг – несанкционированное копирование информации с магнитной полосы платежных карточек (вторые дорожки). Устройство, позволяющее копировать данные с платежных карточек, называется скиммер (рис. 2). Он может содержать в памяти до ста номеров карточных счетов, информация в дальнейшем может быть перенесена на компьютер.

Одним из видов мошенничества является генерация номеров карт и тестирование картсчетов. Цель мошенничества – открытие BIN ranges (STIP и/или Host) и калькуляция проверочной цифры MOD 10. Способом противодействия в этом случая выступают процедуры авторизации, мониторинг и BIN менеджмент.

Рис. 2. Скиммер

Основные угрозы, на долю которых приходится львиная доля ущерба, наносимого субъектам информационных отношений в индустрии платежных карт, представлены на рис. 3.

Растущие потери в индустрии платежных карт привели к необходимости создания единых глобальных стандартов для всех платежных систем. 7 сентября 2006 г. Visa International, MasterCard Worldwide, American Express, Discover Financial Services, Diners' Club, JCB объявили о создании независимого Совета для координации работы по развитию Стандарта безопасности данных индустрии платежных карт (PCI DSS) [5].

Рис.3. Классификация угроз информационной безопасности в индустрии платежных карт

Выводы. Информационная безопасность должна достигаться экономически оправданными мерами с обязательным своевременным оповещением правоохранительных органов о мошенничестве. Предложенная классификация угроз позволяет сопоставить возможные потери от нарушений информационной безопасности со стоимостью защитных средств и выбрать направления, на которых целесообразно сконцентрировать основные ресурсы. Результаты данной статьи в ходе дальнейших исследований могут составить основу для анализа и управления рисками в проектах информационной безопасности. Применение индуктивного и других методов системного анализа позволяет обобщить результаты исследования и перенести их на другие, неэкономические, отрасли нематериальной сферы.

ЛИТЕРАТУРА

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» // www.nbuv.gov.ua/law/07_isu.html.

2. Украинская межбанковская ассоциация членов платежных систем «ЕМА» // http://www.ema.com.ua.
3. Приймак В.М. Прийняття управлінських рішень: навчальний посібник. – К.: Атіка, 2008. – 240с.
4. Галатенко В.А. Основы информационной безопасности.– М.: ИНТУИТ.ру, 2003.– 280 с.
5. Стандарт безопасности данных индустрии платежных карт (PCI DSS). Версия 1.1, 2006 // http://dsec.ru/consult/pcidss/PCI_DSS_v1-1_rus.pdf.

Стаття надійшла до редакції 19.08.2008 р.