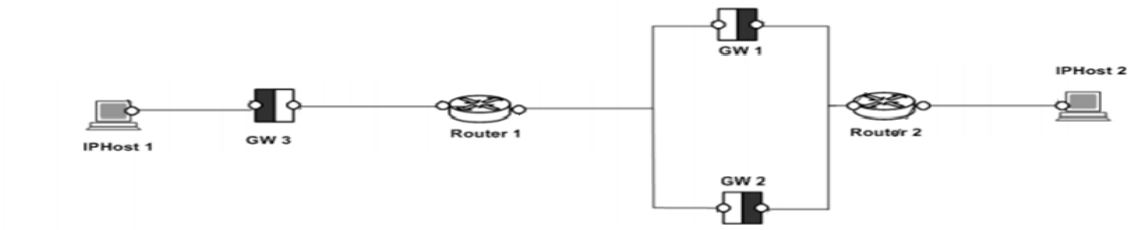

Рисунок 1 – Логика работы отказоустойчивого решения

В предложенном решении реализована следующая логика работы:

– в качестве кластера используются два шлюза безопасности CSP VPN Gate;

– шлюзы имеют различные роли – GW1 – основной шлюз безопасности, GW2 – резервный шлюз безопасности;

– кроме шлюзов безопасности определены два «надежных» устройства. На эти устройства отправляются ICMP-пакеты для диагностики работоспособности сетевых интерфейсов шлюза безопасности;

– в нормальном режиме весь трафик обрабатывается на основном шлюзе безопасности, а резервный шлюз безопасности в это время находится в режиме ожидания;

– в случае выхода из строя основного шлюза безопасности, его заменяет резервный шлюз безопасности и обрабатывает весь проходящий трафик;

– после восстановления работоспособности основного шлюза безопасности резервный шлюз переходит в режим ожидания и отдает управление основному шлюзу безопасности;

– проверка работоспособности основного и резервного шлюзов безопасности, а также действия по активации и настройке интерфейсов производятся с помощью скриптов, устанавливаемых на шлюзы безопасности.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В РЕШЕНИЯХ ПО БЕЗОПАСНОСТИ БАНКОМАТОВ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Никифоров В.В.

Шпак И.И. – канд. техн. наук, доцент

В докладе рассматриваются виды мошенничества с банкоматами. Рассматривается комплекс мер защиты конфиденциальной информации клиента, в частности IPSec, который представляет собой основанный на стандартах набор протоколов и алгоритмов защиты. Однако принимаемые меры не дают сто процентной гарантии, что злоумышленник не сможет завладеть данными.

В современном обществе устройства по обслуживанию пластиковых карт (банкоматы) пользуются всё более возрастающей популярностью. Банковские счета открываются повсеместно. Для надёжного хранения и удобства управления своими деньгами люди пользуются банковскими картами. Согласно оценкам компании Retail Banking Research Ltd, в мире установлено свыше 1,2 млн. банкоматов. Банкомат становится объектом криминальных действий мошенников.

Наиболее распространенными типами атак являются:

Заедание карточки (Cardjamming), подкачка карточки (Cardswapping), компромат по PIN-коду (CompromiseofPINnumber) , вандализм, диверсии [1].

Инновации и возможности человека растут с каждым днем. Производители банкоматов, пытаются делать все возможное для того, чтобы вся конфиденциальная информация была в сохранности. К конфиденциальным данным относиться:

1) номер держателя карты,
2) пин-код
3) CVV-код, используется для проверки подлинности карты.

Так же и сами владельцы банкоматов, а именно банки, стараются оградить клиентуру от различных видов мошенничества. Полностью избежать таких ситуаций, к сожалению, невозможно, потому как злоумышленники так же изобретают различные приспособления, устройства, находят иные способы реализации их планов.

Основные методы хищения носят технологический характер. За многолетнюю практику, в банке «Белгазпромбанк» было зафиксировано множество попыток хищения конфиденциальной информации.

Для этого было решено ввести ряд технических доработок. Так как многие АТМ находятся удаленно от

Библиотека БГУИР

основного сервера банка, отследить вторжение на сетевом уровне достаточно тяжело. Основным мощным внедренным средством, конечно же является аппаратное оборудование Cisco 881-V-K9 и CISCO 871-K9. Эти два устройства выбраны именно потому, что в них используются любые виды алгоритмов шифрования, без конкретизации их стойкости. Именно поэтому почти во всех устройствах Cisco в артикуле присутствует окончание K9. Аппаратные продукты Cisco для поддержки VPN используют набор протоколов IPSec [2].

IPSec представляет собой основанный на стандартах набор протоколов и алгоритмов защиты. Технология IPSec и связанные с ней протоколы защиты соответствуют открытым стандартам, которые поддерживаются группой IETF (Internet Engineering Task Force — проблемная группа проектирования Internet) и описаны в спецификациях RFC и проектах IETF. IPSec действует на сетевом уровне, обеспечивая защиту и аутентификацию пакетов IP, пересылаемых между устройствами

IPSec обеспечивает следующие возможности VPN в сетях Cisco:

1) Конфиденциальность данных. Отправитель данных IPSec имеет возможность шифровать пакеты перед тем, как передавать их по сети.

2)Целостность данных. Получатель данных IPSec имеет возможность аутентифицировать сообщающиеся с ним стороны (устройства или программное обеспечение, в которых начинаются и заканчиваются туннели IPSec) и пакеты IPSec, посылаемые этими сторонами, чтобы быть уверенным в том, что данные не были изменены в пути.

3)Аутентификация источника данных. Получатель данных IPSec имеет возможность аутентифицировать источник получаемых пакетов IPSec. Этот сервис зависит от сервиса целостности [3].

Так же была установлена сигнализация предотвращающая несанкционированное вскрытие сейфа и отсека с оборудованием. Установлены антискиминговые накладки на считыватель карт и видеонаблюдение, затрудняющие установку оборудования злоумышленника.

И даже после принятия таких, казалось бы, крайних мер, злоумышленникам все же иногда удается завладеть данными карты клиента.

ВЫВОД: Принятый комплекс мер защиты конфиденциальной информации клиента, не дает сто процентной гарантии, что злоумышленник не сможет завладеть данными. Принято решение полной комплектации банкоматов средствами различной степени защиты, не зависимо от мест расположения. При появлении нового способа хищения, банки, организации обслуживающие банки, а также их производители, незамедлительно разрабатывают новый метод защиты.

Список использованных источников:

1.Воронин, Алексей. Мошенничество в платежной сфере: «Альпина Паблишер»./ Алексей Воронин - М: 2016.

2. Cisco 880 Series Integrated Services Routers Data Sheet – Cisco [Электронный ресурс]. – Режим доступа: www.cisco.com › ... › Data Sheets. Дата доступа: 27.04.2017.

3.Соммервил, И. Инженерия программного обеспечения. 6-е изд./ И.Соммервил. - М.: Издательский дом «Вильямс», 2002.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Павловский Д.А.

Савенко А.Г. – магистр технических наук, ассистент

Решается задача создания программного комплекса, который позволит сократить время, упростить и автоматизировать процесс поиска патентов и товарных знаков, а также их подачи в различные патентные офисы.

При инновационной и научной деятельности важной составляющей является защита прав на изобретение, полученное в результате данной деятельности. Основным охранным документом в данном случае является патент. Патенты выдаются различными государственными органами исполнительной власти по интеллектуальной собственности – так называемыми «патентными офисами». Для Республики Беларусь – это Национальный Центр Интеллектуальной Собственности, для Японии – Japanese Patent Office (JPO), для Соединенных Штатов Америки – United States Patent and Trademark Office (USPTO). Каждый патентный офис имеет свою собственную форму заявки, что вызывает некоторые сложности при ее подаче.

Основным компонентом программного комплекса является система управления интеллектуальной собственностью, которая решает вышеупомянутую проблему. Подача заявки через систему осуществляется через унифицированную форму, предоставляемую пользователю системой. Форма содержит как общие поля, так и специфические поля, необходимые для подачи заявки в конкретный патентный офис. После заполнения пользователем формы, система осуществляет проверку введенных данных на правильности заполнения. В случае, если форма заполнена верно, то начинается процесс генерации заявки в соответствие с необходимым форматом заявки целевого патентного офиса.

Другой важной функцией системы управления интеллектуальной собственностью является возможность поиска необходимых патентов и товарных знаков. При этом нужно обеспечивать необходимую безопасность для данных. Исходя из этого, необходима поддержки децентрализованной базы данных, которая могла бы храниться в различных экземплярах для разных организаций. В качестве СУБД использована Microsoft SQL Server, использующая в качестве языка запросов диалект Transact-SQL и

Библиотека БГУИР