БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ИНСТИТУТ ИНФОРМАТИКИ, ЩЕЦИНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (ПОЛЬША)
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ
БЕЛОРУССКАЯ АССОЦИАЦИЯ АНАЛИЗА И ОБРАБОТКИ ИЗОБРАЖЕНИЙ

NITE '96

Вторая международная конференция

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

Ноябрь 12-13, 1996

В сотрудничестве с
Министерством образования и науки Республики Беларусь
Технологическим университетом Тройеса (Франция)
Академией наук Беларуси
Университетом Дерби (Великобритания)
Университетом Напиер (Великобритания)
Белорусский государственный университет
Университетом Сантьяго-де-Компостелла (Испания)
Небриссенским университетом (Испания)
Университетом Нис (Югославия)
Международной Академией Информатизации
Белорусским и польским центрами IEE

Минск
Республика Беларусь

Основные проблемы защиты информации в системах телекоммуникаций

Н.В. Пацей, И.П. Урбанович

220630, г. Минск, ул. Свердлова, 13а , БГТУ, тел.2274376, факс 2261075

Аннотация: *Статья посвящена такому актуальному вопросу, как обеспечение безопасности и защиты информации в банковских и коммерческих системах телекоммуникации. Перечислены возникшие на сегодняшний момент проблемы в этой области. Охарактеризованы наиболее общие решения, защищающие вычислительные ресурсы банков и предприятий от угрожающих им опасностей и даны некоторые рекомендации для повышения уровня защиты информации.*

Ключевые слова: *телекоммуникации, информация, банковская система, безопасность, защита, сообщения, сеть, средства, стандарты, инфраструктура шифрование.*

Введение

В последнее время укрупнилась инфраструктура электронной коммерции и электронных банков, как основы электронных платежей. Цифровое банковское будущее развивается с головокружительной быстротой. Оно постепенно переходит в ведение разработчиков программ и будет рассматриваться как одна из форм обработки информации, а деньги - просто как тип данных. Аналитики видят в электронном банковском деле и коммерции целый ряд проблем: отсутствие удобного способа обмена электронными сообщениями, отсутствие законодательных актов и подходящих средств защиты информации. Широкое распространение сетей Internet, SWIFT, национальных и глобальных сетей придают проблеме информационной защиты особую актуальность.

Электронная коммерция ставит проблемы доверия и удобства со стороны потребителей. К сожалению, уровень защиты финансовых транзакций совершенно недостаточен. Отсутствует готовая инфраструктура для обеспечения их безопасности. Необходимо решить проблемы перехода на автоматическое аппаратное шифрование текста сообщений и усовершенствование процедуры автоматического обмена ключами, устранения свойственной сделкам по Internet фрагментарности и предложить пользователям средства аутентификации кредитных карточек в реальном времени, совместного использования разнообразных средств мониторинга и детектирования антивирусного программного обеспечения (ПО), схем обнаружения попыток внедрения извне и журналов регистраций. Другую проблему представляют собой новые штаммы компьютерных вирусов. По-прежнему велика степень риска потери данных. Не удовлетворительно оценивается и безопасность работы в Internet. Серьезные трудности появились при поиске подходящих инструментов и специалистов требуемой квалификации. Хотя разнообразие продуктов защиты информации может ошеломить (сотни брандмауэров, десятки пакетов шифрования), менеджеров сетей не устраивают стандартные тиражируемые решения. Существует и психологический фактор, препятствующий приживаемости средств защиты. С точки зрения рядовых пользователей, работа в условиях секретности, шифрация\дешифрация рабочих данных, ввод многократных паролей оказывается весьма затруднительным[1].

На данный момент существуют коммерческие приложения защиты информации и корпоративные средства, которые разрабатываются организациями самостоятельно. Последним уделяется слишком мало внимания.

2. Основные проблемы и их решения в области защиты информации

Электронная коммерция не получит широкого распространения без соответствующих нормативов на защиту передаваемых данных. Есть немало уязвимых мест в стандартных алгоритмах шифрования. Тем не менее, в этой области ожидаются

реальные сдвиги, которые сделают возможной интерактивную коммерческую деятельность в "промышленном масштабе". Стандарты на средства защиты информации будут способствовать расширению использования Internet, самой перспективной инфраструктуры электронного обмена данными между производителями, заказчиками и поставщиками. Широко применяется специальная технология защиты данных STT, включающая два уровня защиты: один - на границе между потребителем и продавцом, другой - между потребителем и банком. Используется встроенная защита - протоколы SHTTP и SSL, PPTP .

В платформы защиты банковской информации обычно входят средства шифрования, обеспечивающие конфиденциальность во время передачи, брандмауэр и фильтрующие маршрутизаторы безопасности, ограничивающие доступ в систему из внешних сетей и механизмы подтверждения подлинности и идентификации объекта. К базовым технологиям защиты электронных транзакций относятся: шифрование и метод цифровой подписи. Однако ни шифрование, ни средство аутентификации документов - цифровая подпись, не способны радикально решить проблему несанкционированного доступа, хотя и могут служить сильным сдерживающим фактором. Наилучшим способом защиты может быть введение в транзакции некоторой избыточности для реализации механизма квитирования сообщений, что позволит сформировать "электронный след" платёжных операций.

Идёт подготовка спецификации защищённых коммерческих транзакций SET, позволяющая решить проблемы защиты транзакции по кредитным карточкам. Разработаны "интеллектуальные" дебетовые карточки со встроенным микропроцессором, снижающим вероятность мошенничества. Широко применяется ПО защиты пакетов электронного обмена документами EDI по Internet. Уже разработаны программы для контроля удалённых пользователей, способные не только выявить обладателей модемов, стремящихся войти в сеть, но и идентифицировать их [2].

Ни один банк не может стать полноценным членом мирового банковского сообщества, не подключившись к международной финансовой сети SWIFT. По вполне понятным причинам исключительно важное значение в SWIFT придаётся обеспечению безопасности. В сети применяется:

- микропроцессорные карты для подключения терминалов;
- автоматическое отключение терминала системой в ряде случаев;
- нумерация и отслеживание входящих и исходящих сообщений;
- шифрование, в том числе и контекстно-зависимое, текста сообщений;
- создание отчётов об обмене сообщениями;
- завершение сообщения специальным ключом - аутентификатором;
- категорирование пользователей в зависимости от выполняемых функций;
- разграничение привилегий пользователей внутри категорий;
- резервное копирование информации от системных сбоев;
- дублирование дисков;
- резервные терминальные компоненты для дублирования всех транзакций основного комплекса (автоматическая передача управления при аппаратном сбое на основном комплексе);
- поддержка целостности баз данных (журналы транзакций, откат и восстановление данных) [3].

Однако и здесь возникает необходимость синхронизации работы безопасности всех платформ. Был бы весьма эффективен готовый продукт, выполняющий функции универсального средства безопасности для всей компьютерной системы. К сожалению, подобного продукта на рынке пока нет, как нет в природе абсолютно защищённых сетей. Чтобы выработалось чувство безопасности и комфорта в отношении электронной коммерции, необходимо время.

Дело каждой компании - самой решать, какой уровень защиты информации для неё приемлем. Основная рекомендация - спроектированная система защиты должна реагировать на попытки входа во внутреннюю сеть и блокировать их. Для этого, в первую очередь, необходимо оценить степень коммерческого риска, желательно на стадии проектирования системы, не переоценивая опасность потери информации и выявить незащищенные области, используя экспертные системы по оценке риска. Второй шаг - разработка стратегии защиты. Не следует

перегружать сеть средствами защиты и пренебрегать встроенными системами, предусмотренными во многих продуктах. Решение проблемы информационной безопасности должно носить комплексный характер и сочетать в себе стандартные и нестандартные средства. Даже самые надёжные методы защиты не гарантируют абсолютной безопасности. Поэтому необходимо приложить немало усилий, чтобы создать должный уровень защиты информации на каждом сегменте сети, связанном с корпоративным (торговым) клиентом. Защиту телекоммуникаций следует рассматривать как часть общей стратегии безопасности информации. Поэтому исключительно важную роль играют мониторинг, аудит и контроль целостности, использование диагностического и тестового оборудования для выявления отказов и сбоев сети, настройка сети на обнаружение нарушителя. Желательно вести учет инцидентов, связанных с вирусными атаками и их последствий. Это позволит строить правильную политику защиты от вирусов.

Централизованный контроль средств безопасности - самый простой и распространенный метод. Оптимальным решением в этой связи будет создание административной станции защиты, выполняющей настройки политики безопасности для разных компонентов системы, дистанционное регулирование и конфигурирование системы по защите, пассивное и активное воздействие на идентифицированный источник опасности, трансляцию адресов и другие функции.

Корпорации увлеклись средствами защиты от проникновения из глобальных сетей, но не стоит забывать о безопасности ПК и серверов, о восстановлении утерянной информации и физической безопасности. Ведь основная угроза часто исходит не от внешнего, а от внутреннего источника опасности.

Несмотря на то, что компании проводят определённую политику в области безопасности и внедряют разнообразные технологии защиты, все эти меры вовсе не гарантируют полной безопасности их информации. Защита - не только техническая, но и организационная проблема. Ключ в защите данных - информирование каждого сотрудника и пользователя о мерах безопасности. Ответственность за защиту может нести специальное подразделение, сторонняя фирма либо один служащий, специалист по информационной безопасности, в задачу которого входит формулировка плана защиты данных и наблюдение за его исполнением.

Заключение

Из всего вышесказанного можно сделать вывод: защита информации требует постоянного внимания и усилий, и о ней нужно заботиться ежедневно.

Не существует единого мнения, какой набор средств следует считать необходимым, а какой - избыточным. С одной стороны, важно предохранить, а с другой - не перегрузить систему безопасности избыточными мерами. Часто меры по защите информации не требуют излишних усилий, что только увеличивает вероятность того, что система защиты окажется эффективной.

В перспективе, инфраструктура глобальной связи будущего будет включать множество надёжных и защищённых сетей, в том числе и Internet. Сейчас же до полного решения проблем защиты информации в сетях ещё далеко.

Литература

1. Роббинсон Т. Наступает время электронной коммерции //CW, №24, 1996, с.36-37.

2. Роббинсон Т. Как оптимизировать защиту данных в сетях //CW, №15, 1996, с.22-26,47.

3. Большова Д. Международная сеть финансовых сообщений и терминальных комплексов SWIFT//CW, №24, 1996 ,с.41-44.

4. Стенг Д., Мун С. Секреты безопасности сетей. - Киев:Диалектика, 1996 , с.44 .