Обеспечение безопасности банкоматов, систем кассовых терминалов и систем электронного голосования в XXI веке

Безопасность автоматических систем обработки транзакций

S.N. Safe & Software
Опубликовано 1 октября 2009 года

Основные положения

Усиление негативных факторов, влияющих на безопасную работу банкоматов и систем кассовых терминалов, ставит перед производителями оборудования для автоматизированных транзакционных систем задачу обеспечения комплексной безопасности. Сети, ранее работающие на нестандартных аппаратных платформах и операционных системах с использованием специализированных частных сетей, быстро переходят на системы с элементной базой Intel, в которых используются операционные системы Microsoft® Windows® , связанные между собой через протоколы TCP/IP, что увеличивает риск как известных, так и потенциальных угроз.

Традиционные средства защиты от вредоносных программ неспособны обеспечить безопасность банкоматов, систем кассовых терминалов и систем электронного голосования, в большей степени, из-за постоянного появления новых угроз и, как следствие, необходимости частого обновления средств защиты. Кроме того, сложность и количество атак направленного действия неуклонно растет, чему способствует нынешний глобальный экономический спад. Существующие законы и законопроекты содержат требования о принятии всех возможных мер по защите персональной информации; кроме того, в большинстве штатов США необходимо незамедлительно сообщать обо всех случаях утечки данных.

В настоящем докладе рассматривается чрезвычайно неблагоприятная ситуация, возникшая в результате сочетания данных факторов, и необходимость включения средств проактивной защиты данных, таких как Safe'n'Sec TPSecure, в системы обработки транзакций, использующих операционную систему Windows XP. На кону достоверность местных, региональных и общегосударственных выборов, финансовое положение и ценность брендов компаний и наше доверие к выборам и национальным корпорациям. Приемлем ли такой риск?

Чем вызвана необходимость альтернативного подхода?

Ответ прост: необходимость нового подхода к обеспечению безопасности автоматических систем обработки транзакций вызвана, независимо от области их использования, желанием пользователей (как избирателей, так и розничных покупателей или пользователей банкоматов) быть уверенными в защищенности своих персональных данных.

Реальная угроза для бизнеса

17 августа 2009 г. Альберт "Segvec” Гонсалес (Albert “Segvec” Gonzalez) был обвинен федеральным судом присяжных штата Нью-Джерси во взломе серверов пяти компаний, включая Heartland Payment Systems, сети продуктовых магазинов Hannaford Bros. и 7-Eleven. Ранее ему было предъявлено обвинение во взломе серверов TJX Companies, а также шести других компаний розничной торговли и двух ресторанных сетей. Предполагается, что Гонсалес сотрудничал с двумя хакерами, находящимися "в России или соседних с ней странах" и третьим пособником из Майами. Считается, что данная группа похитила более 225 миллионов номеров дебетовых и кредитных карт. 13 сентября 2009 г. Гонсалес признал себя виновным по 20 пунктам обвинения, включая хищение персональных данных, мошенничество с использованием электронных средств коммуникации и преступный сговор. На момент написания данного отчета, остаются открытыми обвинения от 17 августа.

Киберпреступность реальна, это большой бизнес, на котором можно заработать много денег. Недавно сайт *CNNMoney.com* сообщил, что "количество новых сетевых угроз безопасности за последний год выросло почти втрое, достигнув 1,7 млн". Хакеры прибегают ко все более изощренным методам обхода существующих систем безопасности, используя вредоносные программы направленного действия, разработанные для похищения секретной информации в целях обогащения и дальнейшего распространения вирусов, их натиск не выдерживает ни одна сигнатурная система защиты.

Более того, согласно экспертам Канадской ассоциации информационных технологий (ITAC) число программ, предназначенных для кражи персональной информации, в течение следующих нескольких лет может вырасти в десять раз, поскольку преступники воспользуются мировым экономическим спадом, чтобы с помощью финансовых афер обманывать доверчивых и отчаявшихся людей, пообещав им быструю прибыль. Такие люди, — безработные, ищущие простой способ решения проблем, — становятся легкой добычей для кибепреступников.

Используя легальные сайты объявлений о трудовых вакансиях, хакеры набирают группу так называемых "мулов", людей, которые, сами того не ведая, получают и пересылают украденные деньги за небольшую плату. Однако, имеются и осведомленные соучастники, участвующие в обналичивании похищенных денег, снимая их через банкоматы с помощью дубликатов карт, созданных на основе использованных данных. В то же время, создание и модификация вредоносных программ требует все меньших вложений и опыта, что позволяет даже не имеющим глубоких технических познаний преступникам взламывать системы в целях обогащения и проведения комбинированной атаки.

При этом негативные изменения в экономической ситуации влияют и на сотрудников, имеющих доступ к конфиденциальной информации. Сотрудники, раздраженные массовыми увольнениями и неспособные оплачивать свои счета, пользуются уязвимыми местами в информационной инфраструктуре своих компаний, портят программы и данные, либо крадут засекреченную информацию. Информационный центр по преступлениям, связанным с хищением персональных данных (Identity Theft Resource Center, ITRC) отмечает, что в 2008 г. случаев утечек информации, вызванных собственными сотрудниками компаний, было на 47% больше по сравнению с 2007 г. и в четыре раза больше по сравнению с 2005 г.

Большинство сообщений о сетевых атаках на банкоматы поступают из Европы и России, что оказывает успокаивающий эффект на американские компании. Однако, такой подход недальновиден. В своем недавнем обращении Президент Обама отметил, что он считает, что риск сетевых атак представляет собой угрозу национальной безопасности. Он дал понять, что атаки в Европе были приняты к сведению и что было бы наивно полагать, что, учитывая взаимосвязанность мировых финансовых систем, подобные инциденты не могут иметь место в США. Аналитическая фирма Gartner предполагает, что законодательство, регулирующее сферу потребительских товаров, созданных с применением информационных технологий, появится уже в 2011 г. в Европе и в 2015 г. в США.

Несмотря на то, что переход от закрытых систем обработки транзакций к открытым предлагает ряд преимуществ (легкость в использовании, низкая стоимость установки и эксплуатации и т.д.), он создает множество уязвимых мест (это особенно касается автоматических терминалов), что повышает риск известных и неизвестных угроз. Частые обновления и перезагрузки системы, которые необходимы для работы традиционных средств защиты от вредоносных программ в целях обеспечения непрерывной безопасности, просто неосуществимы в автоматических системах, таких как банкоматы, кассовые терминалы, системы электронного голосования. Эффективность традиционных средств защиты, зависящих от обновлений в эпоху все возрастающего количества атак "нулевого дня" является устаревшим решением.

Такие нашумевшие случаи как махинация Альберта Гонсалеса (см. выше) и огромные убытки от сетевых атак начинают вызывать беспокойство у высшего руководства компаний по всему миру.

Размер убытков

Согласно четвертому ежегодному докладу *"Убытки от утечек данных в США"* (*US Cost of a Data Breach Study)* Института Понемона, случаи утечки данных нанесли ущерб американским компаниям в среднем в размере 6,6 млн. долл. США в 2008 г. (до 4,7 млн. долл. США в 2006 г.). Это составляет 202 долл. США на одну взломанную учетную запись. В эту сумму входят такие расходы как стоимость судебно-бухгалтерской экспертизы, штрафы за нарушение стандартов и правил обеспечения безопасности персональной информации (FTC, PCI, SOX и т.д.), требования по компенсации нанесенного ущерба, затраты на замену карты (5-30 долл. США на карту), бесплатные услуги по мониторингу кредитных счетов для пострадавших, затраты на обновление средств защиты и консультации юристов и

специалистов по связям с общественностью. При этом также стоит учесть возможность исков и утрату доверия клиентов, вред, наносимый репутации компании и ценности бренда. Производители систем электронного голосования особенно подвержены риску предъявления исков, которые могут быть поданы в случае простой возможности подтасовки результатов голосования посредством вмешательства в работу системы голосования, что приведет к потере контрактов с государством на высококонкурентном рынке.

В сорока четырех штатах, а также в округе Колумбия, Пуэрто-Рико и на Виргинских островах были приняты законы, обязывающие раскрывать информацию об утечке данных. В большинстве случаев компании, которые владеют, берут в пользование или хранят персональную информацию, должны направить уведомление всем лицам, чьих данных коснулась утечка. Законы предусматривают ряд исключений: например, если украденная информация была закодирована или в случае проведения уголовного расследования, компания не должна раскрывать утечку информации. Имеется еще одна лазейка: в том случае, если украдены номера и PIN-коды карт, но не имена их владельцев, раскрытие информации об утечке не требуется по закону. Однако, в целом, компания, подвергнувшаяся атаке, при которой были похищены или взломаны персональные данные, обязана сообщать о такой утечке. Законы некоторых штатов также предусматривают возможность предъявления гражданских исков о возмещении ущерба за каждый случай нарушения безопасности персональной информации (Калифорния) или по каждому жителю штата, не получившему уведомление об утечке данных (Аляска). И хотя в настоящее время в каждом штате существует собственное законодательство, регулирующее вопросы безопасности персональной информации, Конгресс рассматривает несколько законопроектов, посвященных раскрытию информации об утечке данных на федеральном уровне.

Существующие проблемы

Сети банкоматов

За исключением массового взлома банкоматов Citibank и утечки данных в сети магазинов 7-Eleven, большинство задокументированных атак на банкоматы до настоящего времени происходило в Европе и России. К сожалению, данные инциденты не получили столь широкого освещения в прессе, как в Северной Америке, но такие атаки, вместе с переходом систем банкоматов на операционные системы Windows и появлением программы Zbot/Zeus, указывают на высокую вероятность осуществления взлома банкоматов и в США.

Взлом банкоматов платежной системы RBS WorldPay в 49 европейских городах, когда за 15 минут была украдена сумма, приблизительно равная 9 млн. долл. США, демонстрирует уровень развитости современных киберпреступников. Поскольку такая большая сумма денег была снята со счетов за короткий отрезок времени, предполагается, что хакеры получили доступ через сеть RBS WorldPay и сумели модифицировать ограничения по размеру сумм, разрешенных к снятию со счетов.

В марте 2009 г. компания Diebold сообщила об обнаружении вредоносных программ в банкоматах, установленных в России. Банкоматы, работающие на основе операционной системы Windows, были атакованы и инфицированы тремя троянскими программами, предназначенными для копирования и распечатки информации о кредитных картах и паролях. Хотя данная атака была проведена путем получения физического доступа к банкоматам вместо проникновения через сетевой уровень, установка вредоносных программ могла быть осуществлена только командой опытных киберпреступников, и, что самое важное, такие программы не могли быть обнаружены обычными антивирусными программами.

В начале этого года 20 банкоматов в России и на Украине были заражены вредоносными программами, которые были использованы при атаке на Diebold. На всех зараженных банкоматах была установлена система Windows XP. Учитывая, что для установки вредоносной программы требовался специальный доступ, предполагается, что атака была делом рук инсайдера. Фирма Trustwave, раскрывшая атаку, выявила множество версий данной программы, что со всей вероятностью доказывает, что программа имеет быстро эволюционирующий полиморфный код. Она также может быть использована на других банкоматах, и, согласно результатам Совещания по анализу вредоносных программ, нацеленных на банкоматы (ATM Malware Analysis Briefing), для отражения и выявления будущих атак необходима проактивная защита.

В Западной Европе уже осознали это. В августе 2009 г. Европейское агентство по сетевой и информационной безопасности (ENISA) опубликовало отчет под названием "Преступления со взломом банкоматов: Обзор ситуации в Европе и методы предотвращения". В отчете обращается внимание на растущее число преступлений со взломом банкоматов и приводятся средства защиты от них. По сведениям Европейской группы по безопасности банкоматов (EAST) "количество преступлений со взломом банкоматов подскочило на 149% по сравнению с предыдущим годом". Большинство преступлений совершалось с использованием технологий считывания карт. "Однако, большую тревогу вызывают недавние сообщения об атаках с использованием легкодоступных и продвинутых программ, нанесших удар по сетям банкоматов и самим банкоматам".

Агентство отметило, что наличие нескольких сторон, участвующих в эксплуатации сетей банкоматов, приводит к проблемам коммуникации, в частности, по вопросам безопасности. Часто бывает сложно определить, кто ответственен за проблему. Производители банкоматов должны признать такую ситуацию и взять на себя ответственность за безопасность своей продукции. Также агентство ENISA обратило внимание на особенности конструкции банкоматов, отрицательно сказывающиеся на уровне защиты, в частности на то, что "после установки [банкоматы] редко обновляются и плохо управляются". Кроме того, в соответствии с требованиями, предъявляемым к промышленной продукции, обновления для операционной системы (в основном для Microsoft Windows) сначала должны быть протестированы, сертифицированы и распространены производителем, что создает дополнительные затруднения".

«Учитывая, что отрасль активно переходит с нестандартных систем на более открытую операционную систему Windows XP, наступило время усилить защиту от усложняющихся сетевых угроз, от атак с использованием вредоносного оборудования до атак, приводящих к отказу в обслуживании клиентов. … Мы видим признаки того, что преступники испытывают надежность программного обеспечения банкоматов для того, чтобы найти новые возможности для совершения мошеннических действий. Цель данного руководства – предотвратить действия потенциальных взломщиков программ для банкоматов» – Ассоциация производителей банкоматов (ATMIA), о причинах опубликования «Руководства о передовых методах обеспечения безопасности программного обеспечения банкоматов (ATM Software Security Best Practices Guide) в сентябре 2009 г.

Часто вредоносные коды встраиваются в информационные системы банков через недокументированные сетевые подключения, беспроводные сети без ключей шифрования, необновленные операционные системы или ноутбуки, USB-приводы и прочие портативные устройства. Банковская троянская программа Zbot, которая крадет реквизиты электронных платежных систем, доставляет особенно много неприятностей после попадания в систему благодаря своей способности к трансформации и усовершенствованным механизмам руткита. Исследование фирмы Trusteer, занимающейся Интернет-банкингом, показало, что антивирусные продукты могут обеспечить эффективную защиту против Zbot лишь в 23% случаев. Очевидно, что одного антивирусного программного обеспечения недостаточно. И Zbot лишь одна из сотен тысяч вредоносных программ, существующих в настоящее время.

Мошенничества со взломом банкоматов приводят к большим убыткам. “Секретная служба Министерства финансов США подсчитала, что убытки от преступлений со взломом банкоматов в 2008 г. составили около 1 млрд. долл. США или 350 000 долл. США в день (Отчет "Преступления с взломом банкоматов" агентства ENISA). Помимо упомянутых выше сопутствующих затрат, кредитно-финансовые организации,

подвергшиеся атаке, рискуют столкнуться с оттоком клиентов. По оценкам Института Понемона, в случае утечки данных кредитно-финансовая организация может потерять 5,5% клиентов. Государственные законы о раскрытии сведений об утечке данных требуют, чтобы в большинстве случаев клиент был оповещен о случае утечки, что увеличивает вероятность его ухода к другой кредитно-финансовой организации, к которой он испытывает большее доверие.

Кредитно-финансовые институты нуждаются в таком средстве безопасности банкоматов, обеспечивающем проактивную защиту от атак направленного действия и неразрешенных операций и надлежащую работу сети банкоматов без необходимости частого обновления, перезагрузки или иных действий, требующих физического вмешательства оператора. Такое средство должно работать без перерывов, в реальном времени и без участия оператора, позволяя снизить расходы кредитно-финансовой организации и укрепить доверие клиентов.

Системы кассовых терминалов

Как и сети банкоматов в финансовой сфере, значительная часть кассовых терминалов, используемых в розничной торговле, была переведена со старых систем на операционную систему Windows.
Согласно данным Отчета компании VDC для директоров по информационным технологиям компаний, занимающихся розничной торговлей, в 43% от общего числа систем кассовых терминалов использовалась операционная система Microsoft Windows. В *Отчете по розничным сетям кассовых терминалов в Северной Америке*, подготовленном IHL Group и выпущенном в марте текущего года в 2008 г., 76 % всех новых кассовых терминалов были поставлены с предустановленной операционной системой Microsoft Windows, в 2007 г. этот показатель составлял 71%. Учитывая, что в 2008 г. общее количество поставок кассовых терминалов сократилось на 4,2% увеличение доли ОС Windows на рынке объясняется заменой старых операционных систем на предприятиях розничной торговли, которые пытаются найти легкий способ выполнения Стандартов безопасности данных индустрии платежных карт (Стандарт PCI-DSS).

О необходимости и эффективности стандарта PCI-DSS и содержащихся в нем требованиях о том, чтобы все компании, занимающиеся обработкой платежей с использованием дебетовых и кредитовых карт, обеспечили защиту своих систем от "существующих и вероятных угроз атаки с применением вредоносного программного обеспечения", было написано многое. (Требования и процедуры оценки безопасности, предписанные стандартом PCI DSS, c1.2, октябрь 2008 г.). Данные требования вынуждают как финансовые, так и розничные организации стремительно переходить на новые операционные системы и программы для того, чтобы обеспечить выполнение требований стандартов, под угрозой штрафов со стороны компаний-эмитентов кредитных карт или со стороны федеральных или местных органов в случае утечки данных. *Требование 7. Предоставление доступа к информации о владельцах карт строго с учетом производственной необходимости* обязывает ввести системы контроля доступа, защищающие от непредумышленных ошибок или злонамеренных действий инсайдеров. Кроме того, *Требование 10. Отслеживание и мониторинг всех операций доступа к данным сети и информации о владельцах карт* направлено на максимальное снижение убытков от действий инсайдеров. Данное требование предусматривает ведение контрольного журнала по пользовательским и системным компонентам.

> *«Основное внимание в Стандарте безопасности индустрии платежных карт(PCI) уделяется безопасности программных приложений. За последние несколько лет утечки данных привели к взлому сотен миллионов регистрационных данных. В большинстве из этих случаев межсетевые экраны работали, шифрование работало, велась запись данных, но само приложение содержало пробелы в защите, которые позволили обойти большинство механизмов защиты. Получилось, что главный вход был заперт, но при этом черный ход остался открытым»,* - Онлайновый журнал по вопросам безопасности и рискам CSOonline.com.

Однако, многие другие стандарты неспособны обеспечить защиту интересов клиентов против существующих угроз, которым подвержены системы обработки транзакций. *Требование 5* предписывает

в рамках "программы корректировки недостатков защиты", чтобы пользователи кассовых терминалов "Установили и регулярно обновляли антивирусное программное обеспечение и антивирусные программы … для защиты систем от существующих и вероятных вредоносных программ". Хотя антивирусное программное обеспечение, несомненно, является ценным компонентом любой системы защиты, из-за необходимости частого обновления сигнатур для обеспечения защиты от вирусов и отсутствия защиты от неизвестных и полиморфных вредоносных программ оно не может быть единственной защитой от таких угроз. Кроме того, *Требование 6: Разработать и поддерживать системы безопасности и соответствующие приложения* не содержит требования о том, что сама операционная система должна быть защищенной, также как и внутренние и "общедоступные веб-приложения". Все важные обновления-"заплаты" для обеспечения безопасности должны "устанавливаться в течение одного месяца после выхода". С учетом существующей ситуации один месяц – слишком долгий срок. Необходима проактивная и оперативная защита операционной системы и установленных приложений.

Кроме того, хотя стандарт PCI-DSS предусматривает множество методик защиты персональных сведений в транзакционных сетях, соблюдение данного стандарта не всегда обеспечивает защиту. Например, в истории с утечкой данных в сети супермаркетов Hannaford Bros. была взломана система обработки транзакций компаний, в результате чего было украдено 4,2 млн. номеров кредитных и дебетовых карт, несмотря на то, что в момент утечки, информация о которой была раскрыта в марте 2008 г., в компании соблюдались все требования стандарта PCI-DSS. Атака на Hannaford была дерзкой: вредоносное программное обеспечение было загружено на серверы всех 300 магазинов, затем программа записывала данные каждой кредитной/дебетовой карты при проведении ее через картридер и отправляла данные за границу. В результате тщательного расследования утечки данных в сети Hannaford, а также в Heartland и 7-Eleven было сделано заключение о том, что корпоративные сети всех трех компаний были взломаны с помощью инъекции SQL-кода, что позволило установить программу-анализатор сетевых пакетов ("сниффер"), которая записывала номера дебетовых и кредитных карт в режиме реального времени и пересылала украденные данные через определенные промежутки времени.

Для отражения такого типа атак необходима многоуровневая защита, включающая систему предотвращения утечки корпоративных данных, которая осуществляет мониторинг и контроль сетевых действий всех пользователей, а также проактивный анализ поведения всех приложений и установку последних рабочих версий всех приложений.

Терминалы систем электронного голосования

Если речь идет о терминалах для электронного голосования, перспектива проста: необходимость получить вызывающий доверие результат голосования. Это означает, что:

- Голосующие могут своевременно получить доступ и проголосовать;
- Результаты голосования хранятся в тайне;
- Персональная информация используется только по назначению;
- В результаты голосования не могут быть внесены изменения.

"Часть надежды, которую подает электронное голосование, состоит в том, что с помощью комбинации технологических и процедурных мер по обеспечению безопасности выборы можно будет проводить с большей степенью защиты, чем когда-либо ранее."
- Калифорнийский университет в Беркли

В соответствии с договором с офисом Государственного секретаря штата Калифорния 20-го июля 2007 года Калифорнийский университет в Беркли опубликовал результаты своих исследований, проведенных в рамках комплексного обзора терминалов систем электронного голосования, сертифицированных для использования в Калифорнии. Обзор включал в себя оборудование трех основных производителей систем электронного голосования. В то время как все три поставщика на тот момент обладали необходимыми сертификатами, никто из них не обеспечивал соответствие принципам документа "Добровольные руководящие положения для систем голосования" (Voluntary Voting Systems Guidelines) 2005 года.

Все три вошедших в рамки обзора поставщика (а также большинство остальных) используют для своих Систем управления голосованием и их терминалов операционную систему Windows. После подготовки Системы управления голосованием на базе Windows в избирательном штабе к голосованию она обычно записывается на карты памяти, распределяемые по избирательным пунктам (по одной карте для каждого терминала). На такой карте памяти в ходе голосования записываются все голоса. После закрытия избирательного пункта голоса подсчитываются, карты извлекаются и отправляются в избирательный штаб, где их используют в Системе управления голосованием для составления таблиц.

В рамках анализа Калифорнийского университета в Беркли исследовательской группе легко удалось использовать известные пробелы в системе безопасности операционной системы на оборудовании одного из производителей, несмотря на доступность обновлений-"заплат" для них. В отчете также высказывается предостережение, касающееся того, что при заражении одной из карт памяти и использовании ее при загрузке терминала системы голосования вирус может распространиться на Систему управления голосованием в целом и заразить систему голосования всей страны.

"Добровольные руководящие положения для систем голосования" 2005 года были подготовлены Комиссией по содействию проведению выборов США (US Election Assistance Commission), чтобы предоставить штатам набор требований и спецификаций, которые они могли бы использовать при сертификации своих систем электронного голосования. С учетом того, что в 2005 году в данный документ не были включены рекомендации по мерам защиты, необходимым для обеспечения достоверных результатов выборов, Комиссия подготовила Предварительные требования для "Добровольных руководящих положений для систем голосования" 2007 года, которые в настоящий момент доступны для широкой публики. В Главе 5 данного документа говорится, что системы электронного голосования должны:

- Предотвращать установку вредоносного ПО в системы управления голосованием и терминалы для голосования. В случае внедрения вредоносного ПО, оно может привести к неправильному подсчету или записи голосов, воздействуя, таким образом, на результаты выборов. Оно также может привести к выходу терминалов из строя, препятствуя голосованию граждан;
- Блокировать вирусы, способные перемещаться с одного терминала на другой или с терминала в систему управления голосованием;
- Защищать данные избирателей (тайный характер голосования и персональную информацию);
- Ограничивать сетевой доступ персонала теми приложениями, которые необходимы для исполнения их обязанностей, чтобы предотвратить возможность установки инсайдерами вредоносного ПО на терминалы и/или в Систему управления голосованием или воздействия ими на результаты выборов;
- Записывать все системные события с целью контроля.

Эффективное решение по обеспечению безопасности должно использовать проактивную автоматическую защиту, предотвращающую заражение систем управления голосованием вредоносным ПО, внедренным с помощью съемных носителей или непосредственно через сеть. Потенциальная возможность злонамеренного вмешательства изнутри должна быть исключена с помощью четко определенной системы распределения прав доступа по классам, предоставляющей большое количество настроек и правил доступа к данным для обеспечения индивидуальным пользователям или группам пользователей доступа к информационным ресурсам с точно определенными границами. Необходимо также наличие устойчивой встроенной системы формирования отчетности для мониторинга и записи сетевой активности всех пользователей и создания необходимых контрольных журналов.

Новый подход

На протяжении последних 20 лет решения в области защиты от вредоносного ПО оставались большей частью неизменными. С учетом того, что в лаборатории ежедневно прибывают десятки тысяч образцов новых вирусов, традиционных средств защиты стало недостаточно. Защита, основанная на обновлении сигнатур, операционной системы и программных приложений, на внедрении систем предотвращения вторжений HIPS и даже на применении "белых" списков приложений, перестала обеспечивать

достаточный уровень безопасности сетевых систем обработки транзакций на фоне расширяющегося диапазона и числа угроз, как внешних, так и внутренних.

Пришло время для нового подхода: проактивной, автоматической защиты всех точек системы обработки транзакций от внешних и внутренних угроз, которая становится возможной только благодаря применению контроля над программным обеспечением системы в режиме реального времени, гарантирующего, что в работу разрешенных приложений не сможет вмешаться никто и ничто. Обеспечив безопасную работу приложений, можно гарантировать, что сеть будет непрерывно находиться в исправном состоянии, что она будет защищена от вмешательства в ее работу известных и новых вредоносных программ и что она не станет жертвой утечки данных - случайной или злонамеренно спровоцированной изнутри организации.

Такое решение:

- Защищает данные пользователя;
- Обеспечивает доступность терминальных систем;
- Снижает уровни финансовых рисков;
- Поддерживает ценность бренда и уверенность в нем потребителя;
- Соответствует нормативным требованиям;
- Уменьшает расходы на поддержание безопасности.

Именно таким решением является Safe'n'Sec TPSecure.

Высокий уровень защиты обработки транзакций

Обеспечение соответствия этим критериям - непростая задача. Число возможных угроз для систем обработки транзакций, включая входящие в их состав автоматические терминалы (например, банкоматы, кассовые терминалы и терминалы систем электронного голосования), весьма велико. Для обеспечения высокого уровня безопасности обработки транзакций решение должно защищать всю сеть в целом от:

- Вирусов, червей, троянских программ - вредоносного программного обеспечения, повреждающего или удаляющего информацию системы;
- Программ-шпионов - программ, посылающих данные с терминалов сети третьим сторонам без ведома оператора;
- Руткитов - программ, скрывающих следы деятельности злоумышленников и присутствие вредоносного года на терминале или сервере;
- Клавиатурных шпионов - программ-наблюдателей, записывающих и сохраняющих персональные данные пользователей (например, PIN-коды) и другую конфиденциальную информацию;
- Любых программ, пытающихся скрытно внедриться в систему терминала;
- Хакерских атак, заключающихся в выводе системы из строя и уничтожении данных сети обработки транзакций.
- Несанкционированного внешнего управления сетью обработки транзакций;
- Эксплойтов - злоумышленного использования системы за счет уязвимостей ее программного обеспечения;
- Случайных и умышленных действий инсайдеров - установки вредоносного ПО и уничтожения или хищения конфиденциальной информации.

Более того, решение должно предоставлять все эти возможности без необходимости непрерывного обновления, корректировки и перезагрузки для гарантии работоспособности защиты.

TPSecure: Автоматизированная защита сети в режиме реального времени

Технология проактивной защиты

Продукт Safe'n'Sec TPSecure создан на основе технологии **V.I.P.O.** (Valid Inside Permitted Operations). Технология **V.I.P.O.** объединяет в себе адаптивное профилирование, выполнение приложений в защищенной среде и подсистему поведенческого анализа, гарантируя динамическое проактивное обеспечение целостности приложений. Поддержание безопасной работы приложений в режиме реального времени обеспечивает непрерывное исправное состояние сетей обработки транзакций и защиту от вторжения известных и новых вредоносных программ, включая угрозы "нулевого дня" от внешних и внутренних источников. Поскольку эффективность защиты не зависит от обновлений сигнатур, в управлении системой не требуется оперативность, что создает идеальное решение для автоматических систем, таких как банкоматы, кассовые терминалы и терминалы систем электронного голосования. После установки и приведения системы в исходное исправное состояние администрирование в операторском режиме больше не требуется. Система может автоматически блокировать атаку, поскольку для восстановления оборудования и возобновления его работы не требуется перезагрузка.

Технология **V.I.P.O.** предназначена для предотвращения возможности внедрения вредоносного ПО в операционную систему и запуска несанкционированных программ на одном или нескольких терминалах. Технология **V.I.P.O.** основана на перехвате вызовов системных функций на уровне ядра операционной системы (Кольцо 0) и загружается раньше всех остальных приложений. Она позволяет идентифицировать, анализировать и, при необходимости, блокировать доступ к файловой системе и объектам системного реестра, к запуску приложений и к другим операциям сетевого графика, потенциально способным воздействовать на целостность приложений. Технология **V.I.P.O.** создает защиту ядра операционной системы для предотвращения запуска вредоносного кода. Она олицетворяет собой принципиально иной подход к вопросам информационной защиты - максимально соответствующий нуждам современных сред обработки транзакций.

Предотвращение выполнения несанкционированного кода, пытающегося внедриться в операционную систему, достигается при помощи создания изолированной среды - виртуальной "песочницы" (sandbox). В ней код может выполняться безопасно для вычислительной системы, не воздействуя на другие ее части. На практике это означает, что вредоносное ПО не может получить доступ к операционной системе, разрешенным приложениям или буферу обмена данными для внедрения перехватчиков, клавиатурных шпионов и другого потенциально опасного кода. Это также означает невозможность изменить код и данные, принадлежащие другим процессам, а также несанкционированно модифицировать исполняемые файлы.

- Сканирование системы и профилирование каждого из приложений в операционной системе;
- Составление списка приложений, заслуживающих доверия;
- Поддержка функционирования системы в строгом соответствии со всеми заданными правами доступа;
- Предотвращение запуска потенциально вредоносных приложений;
- Исполнение приложений только с надлежащими правами.

Технология **V.I.P.O.** использует стабильные алгоритмы хеширования, позволяя зарегистрированным пользователям управлять файловой системой и системным реестром, а также обеспечивая целостность файлов и установленных приложений системы. Она позволяет осуществлять запуск только априорно благонадежных приложений. Запуск неопознанных приложений невозможен до тех пор, пока пользователь с соответствующими правами не укажет степень доверия к этому приложению. Технология **V.I.P.O.** также контролирует и блокирует запуск неопознанных исполняемых модулей, что

предотвращает систему от заражения через пробел в защите благонадежного приложения. Самообучающаяся система оптимизирует защиту обычных рабочих процессов и функций.

Уникальные выгоды благодаря использованию TPSecure в системах обработки транзакций

- **Легкость защиты терминала** посредством удаленной или локальной установки (включая возможность использования "беззвучного режима") с помощью программы Microsoft Installer®. Эти функциональные возможности существенно повышают производительность операторов терминалов (банкоматов, кассовых терминалов, терминалов систем электронного голосования).
- **Активация и лицензирование терминала** через Интернет.
- **Возможность настройки графического пользовательского интерфейса** для любого размера экрана, что облегчает использование системы на широком спектре различных терминалов.
- **Обнаружение и предотвращение запуска вредоносного ПО** на съемных носителях.
- **График доступа к системным ресурсам** позволяет выделить для обслуживания терминалов специальные периоды времени, повышая защиту от несанкционированного доступа.
- **Управление файлами с использованием подстановочных символов** существенно упрощает настройку системы (например, возможность запретить изменение всех файлов с именем *.doc).
- **Контроль доступа пользователей/групп** обеспечивается посредством администрирования в режиме конфиденциальности информации с помощью четко определенной системы распределения прав доступа по классам, основанной на политике компании. Наличие большого количества настроек и правил доступа к данным предоставляет индивидуальным пользователям или группам пользователей многоуровневый доступ к информации.
- **Запрет доступа к системным ресурсам** для всех приложений, кроме специально выбранных, существенно упрощает настройку системы.
- **Централизованная запись и формирование отчетов обо всех системных событиях**.
- **Мониторинг в теневом режиме** обеспечивает постоянное присутствие программного обеспечения на рабочей станции пользователя. Оно не может быть обнаружено или удалено.*
- **Администратор контролирует все действия пользователя**, будь это работа в сети, доступ к сетевым ресурсам или к передаваемым данным. Вся действия, связанные с копированием данных, контролируются в теневом режиме, как и все файлы, копируемые на съемные носители.*
- **Запись снимков экрана** обеспечивает возможность просмотра и записи состояния экрана пользователя в любой момент для выявления случайной и умышленной активности инсайдеров - как в онлайн-режиме, так и в ходе ретроспективного анализа.*
- **Использование малого количества ресурсов и места в памяти** обеспечивает минимальные требования к производительности.

* *Данные возможности могут быть активированы/деактивированы с помощью лицензионного ключа, чтобы обеспечить соответствие местному законодательству и политике компании.*

Заключение

Для защиты сетей обработки транзакций от возрастающего числа угроз в наши дни недостаточно полагаться на одно или два средства безопасности. Критическое значение приобрел многоуровневый подход, при котором в сочетании с мониторингом и контролем программного обеспечения в режиме реального времени используются межсетевые экраны, антивирусное ПО, системы предотвращения вторжений HIPS и обновления операционной системы. Идеальным решением является система, сочетающая проактивный поведенческий анализ, выполнение приложений в защищенной среде и адаптивное профилирование, что гарантирует исправную работу приложений системы обработки транзакций.

Аналитики компании Gartner с этим согласны. В сентябре 2009 года в отчете "Исследование рынка - Распознавание структур с помощью технологий мониторинга для обеспечения безопасности и обнаружения мошенничества" они утверждают, что:

- Проведение атак направленного действия требует широкомасштабного мониторинга активности пользователей и возможности распознать те последовательности действий, которые сигнализируют о нарушении обычного поведения и доступа к ресурсам.
- Ненадлежащее использование сотрудниками своих прав требует мониторинга исключений в моделях поведения пользователей, а также контекста ресурсов и ролей.
- Предотвращение мошеннической деятельности требует использования подхода, основанного на математическом прогнозировании и/или оповещениях, генерируемых в соответствии с определенной системой правил, который позволит вести наблюдение за пользователями, учетными записями, транзакциями и другими заданными единицами на предмет обнаружения "аномального" поведения и свойств.
- Предотвращение несанкционированного доступа к конфиденциальным данным и их перемещения требует использование технологий распознавания шаблонов конфиденциальных данных совместно с политикой контроля доступа.

Для сетей банкоматов, систем кассовых терминалов и систем электронного голосования таким решением является продукт Safe’n’Sec TPSecure.

О компании S.N. Safe & Software

Компания S.N.Safe&Software была основана в 2006 году в результате выделения направления «Проактивная система защиты компьютеров» в рамках компании StarForce, являющейся лидером в сфере защиты программного обеспечения и цифрового контента от копирования и взлома.
Сегодня компания S.N.Safe&Software – это признанный полноправный игрок рынка компьютерной безопасности, имеющий развитую дистрибьюторскую сеть в России и 16 странах мира.
Программное обеспечение Safe`n`Sec® уже используется тысячами владельцев персональных компьютеров и инсталлировано на предприятиях военно-промышленного комплекса, авиационной промышленности, машиностроения и ряде государственных структур.