Уникальный "тонкий клиент"

Сергей Панов, *заместитель генерального директора по производственной деятельности АО "ЭЛВИС-ПЛЮС"*
Сергей Акимов, *заместитель генерального директора АО "ЭЛВИС-ПЛЮС"*

Новая разработка компании ЭЛВИС-ПЛЮС представляет собой аппаратно-программный комплекс, обеспечивающий защищенный доступ к корпоративным ресурсам и поддерживающий ЭП, сертифицированный ФСБ России по классу КС3. В интервью редакции журнала Information Security заместитель генерального директора по производственной деятельности С.Б. Панов и заместитель генерального директора компании ЭЛВИС-ПЛЮС С.Л. Акимов рассказывают о том, как и зачем был создан АПК "ЗАСТАВА-ТК".

– Как на сегодняшний день обстоит дело с требованиями безопасности ИТ? Меняются ли подходы к предотвращению угроз?

С.П.: За последнее время ИТ-ландшафт кардинально изменился. Количество и качество цифровых сервисов растут взрывообразно и в основном все больше и больше ориентированы на конечного пользователя. По своему информационному наполнению и связанности современные цифровые услуги являют собой нечто беспрецедентное. Ведущие банки, например, не просто предлагают своим клиентам оформлять кредитные договоры в режиме онлайн, но и предоставляют расширенные услуги, включающие в себя не только проработку связанных с кредитованием вопросов юридического и коммерческого характера, но и целевые услуги, связанные с созданием бизнеса.

Соответственно, меняются и требования к информационной безопасности. Непрерывное развитие и взаимопроникновение цифровых услуг обуславливают необходимость передачи и обработки огромного количества информации, осуществляемых большим числом связанных между собой различных ИС. В таких условиях риски возникновения угроз ИБ не могут не изменяться – они также растут и изменяются качественно и количественно.

В отношении ЦОДов уровень требований защиты данных, передаваемых и обрабатываемых размещенными там системами, многократно возрастает. Например, ИС, входящие в комплекс госуслуг, могут иметь не только различные интерфейсы и форматы данных, которые надо совместить, но и отличаться требованиями в отношении информационной безопасности. Эти требования необходимо подвести под некий общий знаменатель, на базе которого возможно обеспечить защиту, достаточную для того, чтобы не подвергать риску обрабатываемые чувствительные данные.

Растут и скорости передачи данных. Сегодня иметь канал пропускной способностью 10 Гбит/с – норма жизни даже для сравнительно небольшого офиса. Это, соответственно, определяет требования в отношении производительности средств защиты, в частности шифрования. Кроме того, на фоне повсеместного распространения методов и технологий обработки "больших данных" нельзя не отметить, что эти самые методы и технологии давно и широко применяются в сфере ИБ. Объемы данных управления ИБ и событиями безопасности растут быстрыми темпами, и тем насущнее проявляется потребность в эффективных системах управления СЗИ и высокопроизводительных системах обработки событий ИБ, системах управления инцидентами и поддержки принятия решений.

– Как за последние несколько лет изменились взгляды заказчиков? Что для них стало актуальным?

С.А.: Сегодняшние ИТ-реалии: виртуализация, облачные сервисы, BIG DATA, широкое использование мобильных технологий и т.д. – открывают принципиально новые возможности для бизнес-пользователей, и в большинстве случаев заказчики успешно их реализуют. Эта ситуация, безусловно, отражается и на рынке информационной безопасности, усложняя и без того непростые задачи, стоящие перед безопасниками. И все это в условиях сложной экономической ситуации, недофинансирования, недостаточного кадрового обеспечения и т.д.

Вспоминая последние нашумевшие атаки, хотелось бы отметить, что в значительной мере вызванные ими последствия можно было бы минимизировать, если пользователи на местах своевременно установили бы соответствующие обновления.

Современные ГИС федерального масштаба насчитывают десятки тысяч пользователей. Список таких ГИС, регистрируемых в соответствующих реестрах Минкомсвязи, непрерывно растет, особенно в последние годы. И если в головном офисе проблема ИБ для многих организаций практически решена, во всяком случае, созданы предпосылки к ее решению (имеются необходимые ресурсы, технические средства, квалифицированный персонал, создана система контроля и т.д.), то на местах, в регионах, особенно на рабочих местах рядовых бизнес-пользователей, а их число, напомню, может достигать десятков тысяч, ситуация далека от совершенства. Ожидать своевременного и повсеместного внедрения полученных из центра обновлений, реагирования на угрозы, проведения каких-то регламентных работ персоналом, который далек от выполнения не свойственных ему функций и задач и не имеет соответствующих навыков, не приходится.

Поэтому централизация системы ИБ, с применением средств защиты с максимально облегченной процедурой эксплуатации и обслуживания, в частности имеющих возможность удаленного обновления ОС по доверенным каналам передачи данных, а также перенос нагрузки по обеспечению безопасности в головные офисы, где соответствующие условия созданы, сегодня становятся одной из приоритетнейших задач. При этом мы стремимся к тому, чтобы сделать все процессы абсолютно прозрачными для конечного пользователя, максимально исключив человеческий фактор из процесса обеспечения ИБ – поль-

зователи должны заниматься своими бизнес-задачами и не отвлекаться на непродуктивную с точки зрения бизнеса деятельность. Это лишь повысит производительность и эффективность их труда, сократит издержки, а значит, принесет определенный экономический эффект, получение которого в современных условиях для многих компаний становится не только актуальной, но и приоритетной задачей.

– В июле этого года вы завершили разработку аппаратно-программного комплекса "ЗАСТАВА-ТК". Что он из себя представляет? Какие проблемы заказчика он решает?

С.П.: АПК "ЗАСТАВА-ТК" разрабатывался нами с прицелом на централизацию как ИТ-сервисов, так и сервисов ИБ, позволяющую снизить издержки при эксплуатации территориально распределенных сетей, сетей федерального масштаба. Соответственно, архитектура решения предполагает централизованное размещение максимального числа сервисов и использование технологий виртуализации, в том числе Virtual Desktop Infrastructure (VDI), а также консолидацию в рамках ЦОД приложений управления соблюдением требований регуляторов (Compliance).

В результате у нас получилось простое и крайне эффективное устройство. В нем реализованы функции защиты от НСД, с использованием отечественной ОС Альт Линукс СПТ 7.0, сертифицированной ФСТЭК России. Аппаратная часть, базирующаяся на прошедшей исследования платформе ТОНК 1402 в защищенном от вскрытия исполнении, у нас получилась максимально надежной и реализованной с полным соблюдением требований регулирующих органов, что позволило сертифицировать наше решение в ФСБ России. Нам также удалось значительно упростить и удешевить аппаратную платформу, в частности отказавшись от электронного замка, без ухудшения характеристик устройства.

В качестве VPN-клиента используется наш продукт "ЗАСТАВА", который мы давно и успешно разрабатываем и производим. Данный клиент полностью готов к работе в централизованных системах, для него имеется комплекс средств удаленного управления. С помощью такого комплекса можно управлять десятками тысяч удаленных VPN-клиентов, а также централизованно обновлять ОС удаленных АПК "ЗАСТАВА-ТК" и специальное ПО, обеспечивающее доступ к прикладным сервисам. С нашим устройством также интегрирован механизм ЭП на основе российских смарт-карт E-smart с неизвлекаемым ключом, которые помимо безопасности обеспечивают и персонализацию доступа. Если по каким-то причинам конкретный АРМ у пользователя выходит из строя, пользователь может заменить его и с помощью смарт-карты снова войти в систему, чтобы продолжить работу с того места, где она прервалась.

Для таких ГИС как, например, сервисы МФЦ, ЗАГСы, ePH, ПФР и другие, которые распределены по всей стране и в которых зачастую отсутствуют квалифицированные администраторы ИБ, наше решение чрезвычайно удобно. Устройство достаточно подсоединить к сети, включить, вставить смарт-карту, ввести PIN-код – и оно готово к работе! При этом, повторяю, обеспечено соблюдение всех требований регуляторов. Заказчик получает техническую возможность для работы с ГИС, имеющими высокий класс защиты К1 (ФСТЭК России) и КС3 (ФСБ России). В этом смысле наше устройство уникально – пока аналогов на рынке у него нет. В устройстве обеспечивается поддержка ЭП высокого класса защиты (КС3) и прозрачное централизованное обновление как системного, так и прикладного ПО без участия администраторов на местах эксплуатации.

Техническое обслуживание АПК "ЗАСТАВА-ТК" не представляет какой-либо сложности: неисправное устройство может быть заменено на новое, при этом не требуется дополнительных настроек. Все необходимые для работы настройки и обновление ПО пользователь получает автоматически при входе в систему и подключении к ЦОД.

– В чем основные преимущества "ЗАСТАВЫ-ТК"?

С.А.: Наше изделие является законченным и самодостаточным решением. Все входящие в его состав компоненты взаимоувязаны и органически дополняют друг друга, их рациональное использование позволило обеспечить реализацию требований по информационной безопасности минимальным составом средств и элементов защиты, максимально облегчить процедуру эксплуатации и обслуживания терминальных станций, повысить надежность и гарантированный срок эксплуатации изделия. Ничего лишнего, вес и габариты тоже минимальны. Изделие вводится в работу практически "из коробки", не требуя от пользователя высокой квалификации. И, наконец, обновления, про которые я сегодня неоднократно вспоминал. В АПК реализован совершенно новый механизм установки обновлений, ранее не применяемый в линейке продуктов "ЗАСТАВА", плюсы от использования которого будут наиболее ощутимы в удаленных регионах, на каналах связи с низкой пропускной способностью. Наше техническое решение существенно уменьшает объемы передаваемых обновлений и время на их доставку, а значит, и нагрузку на сети при массовом обновлении.

– Кто является основным потребителем данного АПК?

С.А.: Надеемся, что изделие будет востребовано в государственных и корпоративных территориально распределенных информационных системах и компьютерных сетях, в которых требуется обеспечить централизованную обработку, хранение и доступ к данным с использованием облачных технологий и VDI с высокой степенью защищенности. Если говорить про сценарии использования, то решение, на мой взгляд, будет интересно для:

- обеспечения защищенного удаленного доступа к корпоративным ресурсам из удаленных офисов;
- организации рабочих мест банковских служащих, сотрудников кадровых служб и бухгалтерии, работающих с конфиденциальной информацией.

– Импортозамещение в ИБ-сегменте началось еще до осложнения отношений с рядом стран Запада. Однако сейчас "сделано в России" стало важным критерием выбора продукта или решения, особенно для государственных структур, а у отечественных разработчиков появился дополнительный стимул "догнать и перегнать" западные компании. Как импортозамещение повлияло на вашу компанию?

С.А.: ЭЛВИС-ПЛЮС традиционно занимается криптографией, а это рынок, который жестко контролируется государством, и это правильно. Так было и будет всегда, и тут для нас мало что изменилось.

– Сейчас наблюдается тенденция к партнерству компаний по различным направлениям для совместных разработок. Есть ли в вашей практике примеры такой коллаборации?

С.П.: Возвращаясь к импортозамещению, можно отметить, что наш продукт является ярким примером результата совместной работы российских компаний. Мы за год не только разработали, но и сертифицировали устройство в ФСБ России, во многом благодаря тому, что нашими партнерами были отечественные компании, которые отнеслись к нашей совместной работе очень профессионально.

– Спасибо за беседу!

NM
АДРЕСА И ТЕЛЕФОНЫ АО "ЭЛВИС-ПЛЮС" см. стр. 56