Александр НОВОЖИЛОВ:
«Невозможно отмахнуться от угроз АСУ ТП»

Сейчас в России как никогда раньше оказались востребованы системы контроля доступа и действий пользователей с привилегиями. Эти решения позволяют контролировать работу аутсорсингового персонала и удаленных сотрудников.
Чтобы выяснить главные тенденции использования систем контроля действий администраторов в промышленных системах, мы задали несколько вопросов Александру Новожилову, генеральному директору ООО «АйТи Бастион». Компания является разработчиком системы контроля действий поставщиков ИТ-услуг СКДПУ НТ, работает на рынке 8 лет и реализовала более 100 проектов, в том числе и в АСУ ТП критически важных объектов.

– Какие события прошедшего года, по вашему мнению, оказали наибольшее влияние на рынок средств защиты АСУ ТП?

– Проблематика защиты АСУ ТП вышла на новый уровень. Ее начали активно обсуждать главы государств. Также произошел ряд инцидентов, которые продемонстрировали всему миру реальные экономические и социальные последствия. Оказалось, что даже атаки на предприятия пищевой промышленности могут стать и становятся событиями, на которые обращает внимание весь мир. Сегодня невозможно отмахиваться от угроз, связанных с АСУ ТП.

Усугубила ситуацию пандемия. В связи с переводом сотрудников на удаленный режим работы многие заказчики осуществили экстренную закупку решения. Зачастую мы шли им навстречу и предоставляли систему во временное пользование бесплатно. Конечно, крупные инсталляции проводились на фоне готовности заказчиков впоследствии приобретать решение. Сейчас, в момент обострения международной обстановки, мы вновь готовы оперативно предоставить временные лицензии объектам КИИ, которые укрепляют свою инфраструктуру в авральном режиме. Это предложение имеет огромный спрос.

– Какие угрозы и риски, связанные с СКДПУ НТ, на практике получили наибольшее распространение? Какие ресурсы подвергаются атакам в первую очередь?

– Угрозы и риски, которые СКДПУ НТ позволяет снизить или исключить, обозначены давно, и мы говорим о них постоянно. Поэтому не буду повторяться. Как правило, система работает проактивно, она препятствует реализации угроз, проведению атак в зародыше. Подверженность атакам и угрозам мы скорее видим на примере предприятий и организаций, не внедривших качественную систему этого класса. Инциденты в них часто становятся достоянием общественности. Это и утечки разнообразных важных данных, и получение несанкционированного доступа к критичным системам. В случае АСУ ТП это осуществляется в целях нарушения функционирования систем, а также создания возможностей для таких действий впоследствии.

Что же касается наших заказчиков, то мы в первую очередь узнаем о пользе нашей системы в целом. Также мы можем судить о каких-то деталях, получая запрос на доработку функционала либо шаблонов правил. Информация о конкретных инцидентах, даже если нам о них станет известно, не может быть предметом публичного обсуждения.

– В последнее время отечественные компании на этом рынке заявили о создании целого ряда коллабораций? Что вы думаете и/или предпринимаете по этому поводу/в этом направлении?

– Мы не остались в стороне от этого тренда. Скажу больше, мы занялись взаимодействием с другими отечественными производителями несколько лет назад. Идея очень простая и эффективная при должной реализации. Кто-то силен в одном аспекте, кто-то в другом. Один производитель не может реализовать полный спектр решений даже при наличии неограниченных

ресурсов, так как происходит размытие фокуса, нужно искать компетенции по всем направлениям, что сложно. Недаром в последнее время крупные международные корпорации приступили к переходу от высокоинтегрированных компаний к форме конгломерата отдельных специализированных бизнес-единиц. Таким образом, каждый занимается своим делом, в котором он лидер, а интеграция с другими продуктами позволяет создавать экосистему, которая, функционируя совместно, показывает значительно большую эффективность, чем элементы по отдельности.

Сейчас у «АйТи Бастион» более 10 технологических партнеров, и этот список постоянно пополняется.

Сейчас у «АйТи Бастион» более 10 технологических партнеров, и этот список постоянно пополняется. СКДПУ НТ подтвердил технологическую совместимость сразу с несколькими продуктами «Лаборатории Касперского», Positive Technologies, а также с решениями CyberLimpha, РуТокен, Мультифактор и другими.

– Какие основные аспекты миграции на отечественные решения вы бы выделили? На что рекомендовали бы обратить внимание при выборе решения и поставщика?

– На мой взгляд, в первую очередь стоит обращать внимание на продукты компаний, где работают люди «с горящими глазами». Если люди любят свой продукт, готовы его развивать, то в какие-то разумные сроки продукт приобретет и зрелость, и широкий функционал. При любом выборе в большинстве классов систем вы получите продукт, не вполне соответствующий к тому, к чему вы привыкли ранее. Поэтому ставку стоит делать на более перспективные. К тому же в этом случае заказчик выступает «бизнес-ангелом». Возможно, факт вложения усилий в развитие перспективных продуктов будет греть душу.

Второй крайне важный аспект – наличие у производителя надежной и оперативной техподдержки. На это не всегда обращают достаточно внимания. Это выглядит странно, поскольку в случае прекрасного продукта и плохой поддержки вы потеряете больше, чем в обратной ситуации. Мы в «АйТи Бастион» уделяем огромное внимание работе техподдержки, она у нас одна из лучших на рынке – об этом нам сообщают заказчики.

– Какие технологии в защите АСУ ТП кажутся вам наиболее востребованными в течение ближайших двух лет?

– На мой взгляд, важным остается вопрос защиты от некорректных (в том числе преднамеренных) действий привилегированных пользователей. Этому есть несколько предпосылок. В связи с растущей международной напряженностью снижается доверие к услугам аутсорсеров, в первую очередь работающих с территорий иностранных государств. Компании могут оставаться лояльными своим заказчикам, но никто не застрахован от того, что сотрудник не впадет в нестабильное психоэмоциональное состояние и не начнет осуществлять личную вендетту исходя из собственных представлений о действительности. Впрочем, это касается и фрилансеров, и внутренних сотрудников компании. Вторая предпосылка – кадровый голод в ИТ. Необходимость контроля качества и дисциплины работы сотрудников повышается постоянно. Третья предпосылка – усиление влияние служб ИБ, что обусловливает увеличение количества конфликтов со службами ИТ. Средства быстрого и справедливого разрешения конфликтов становятся все более необходимыми.

– В продолжение предыдущего вопроса: в каком направлении развиваете функционал продуктов – в направлении проактивной защиты, реактивных инструментов или средств протоколирования и расследования инцидентов?

– Прозвучит банально, но во всех направлениях. Мы расширяем возможности системы по сбору разнообразных данных, частично с помощью расширения собственного функционала, а также с помощью углубления интеграции с продуктами партнеров. Вы это назвали коллаборацией.

Возможности проактивной защиты также расширяются. Это отчасти следствие работ по предыдущему пункту. Еще нам помогают запросы наших заказчиков на новые фильтры и правила. Международный опыт в этой области также становится важным источником идей.

Большие шаги вперед позволяет делать наша, не побоюсь этого слова, уникальная система мониторинга и расследования инцидентов. Подобного функционала нет ни у одного решения такого класса, что и обусловливает его ценность для заказчиков по всему миру.

– Как вы видите развитие компании «АйТи Бастион» в 2022 году?

– Мы продолжим развивать нашу линейку продуктов. Если хватит ресурсов, обратим внимание на освобождающиеся ниши и не обязательно только в сфере защиты информации. Работы по импортозамещению предстоит много, есть достаточно тем, которыми сейчас стоит заняться. ■