Сергей БОЧКАРЕВ:

«Защищаться от внутренних угроз необходимо так же осознанно, как от внешних»

В этом году «АйТи Бастион» – лидер российского рынка систем PAM (Privilege Access Management) – отмечает десятилетие с момента основания. За время существования компания реализовала свыше 250 проектов. Сегодня «АйТи Бастион» предлагает сертифицированные продукты для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам. О том, почему защита доступов сегодня актуальна как никогда, и как обезопасить инфраструктуру от кибератак, рассказал генеральный директор «АйТи Бастион» Сергей Бочкарев.

– Десять лет – важный и серьезный рубеж для ИТ-компании. Расскажите, как «АйТи Бастион» сегодня ощущает себя на рынке информационной безопасности?

– Наверное, лучшая оценка – это цифры и их динамика от года к году. Финансовые показатели «АйТи Бастион» растут. За 2023 год выручка увеличилась на 48%, оборот компании превысил 1,78 млрд руб., количество заказчиков выросло на 68%. На наш флагманский продукт – систему контроля и мониторинга привилегированного доступа СКДПУ НТ – растет спрос, причем портфель от госзаказчиков федерального и регионального уровней по итогам года увеличился вдвое. Для государственных структур наши продукты СКДПУ НТ становятся стандартом обеспечения безопасного доступа к критически важным системам. Мы ведем активную работу с профильными министерствами и ведомствами, чтобы удовлетворить запросы и соответствовать требованиям разных инфраструктур.

Вслед за госсектором по числу заказчиков в общей структуре идут банки и финансовые организации, на третьем месте – предприятия нефтегазовой отрасли. В 2023 году усиливаться PAM-системами начали организации транспортной сферы и связанные с информационными технологиями. Растет спрос на СКДПУ НТ в странах СНГ и дальнего зарубежья.

Анализ рынка система привилегированного доступа за прошлый год говорит о том, что большинство организаций приобрело средства контроля доступа ИТ-администраторов впервые, а значит, заинтересованность в решениях такого класса есть, и спрос будет увеличиваться. Интерес к PAM-системам, в частности, обусловлен готовящимся изменением законодательства об оборотных штрафах за утечки персональных данных.

Вместе с рынком растем и мы. Заказчиков стало больше, их запросы усложнились, поэтому команда разработки «АйТи Бастион» тоже расширяется. Наш коллектив за год вырос на 73%, в Москве открылся новый офис компании на 2000 кв. м. В 2023 году мы подписали соглашение о долгосрочном сотрудничестве с Московским политехническим университетом и дали старт полноценной программе стажировки. Положительные результаты в формировании профессиональной команды уже есть, поэтому мы продолжим работать со студентами, нацеленными на ИБ.

– Почему вам как экспертам в защите привилегированного доступа важно и интересно работать с АСУ ТП ЗО КИИ?

– Такие системы подвержены рискам, ведь они играют решающую роль в контроле и мониторинге производственных процессов на значимых объектах в различных отраслях, и это делает их главной мишенью для потенциальных целевых атак. Угрозу АСУ ТП могут нести небезопасные конфигурации ПО, разделение задач между сотрудниками и поставщиками, использование устаревших технологий. Чтобы достичь высокого уровня ИБ, требуется активное и профессиональное участие операторов, интеграторов и поставщиков.

– Иными словами, АСУ ТП – это слабое звено?

– Нарушение безопасности систем типа DCS/SCADA имеет первостепенное значение из-за их критичности и потенциальных последствий успешных атак. «Закрепиться» в АСУ ТП – одна из главных целей злоумышленников. Ведь их компрометация предоставляет привилегированный доступ к внутренним операционным процессам, что с высокой долей вероятности приведет к нарушению

или перехвату контроля операционными процессами критической инфраструктуры.

Проблема стала очевидной для всех, а не только для сообщества специалистов ИБ, в 2017 году. Тогда, напомню, мир впервые столкнулся с применением вируса Triton – вредоносного кода для атак на промышленные системы управления, созданного специально, чтобы подвергнуть опасности жизни тысяч людей.

С каждым годом защищенность АСУ ТП растет, появляются новые обязательные функции – по контролю доступа, логированию и аудиту безопасности. Но даже когда продукт поддерживает самые жесткие стандарты ИБ, реализация функций безопасности не может гарантировать всестороннюю защищенность.

Нарушение безопасности систем также может произойти еще на этапе развертывания. Даже при грамотно составленном техническом задании играет свою роль проблема с разделением обязанностей и ответственности по обеспечению безопасного внедрения.

– Расскажите, чего заказчики ждут от продуктов «АйТи Бастион, когда речь идет о работе с АСУ ТП значимых объектов?

– Заказчики хотят не только мониторить активность привилегированных учетных записей, но также контролировать и управлять доступом. К отрасли пришло понимание необходимости защищаться от внутренних угроз (применять модель нулевого доверия) так же осознанно, как от внешних.

– Какие решения для защиты привилегированных доступов АСУ ТП в КИИ есть у «АйТи Бастион»?

– Наше решение СКДПУ НТ – это комплексная платформа контроля и мониторинга удаленных пользователей и доступов, как привилегированных, так и обычных. Система позволяет не только зафиксировать действия пользователя в сессии, но и сформировать поведенческую модель, а также выявить аномалии и отклонения от нормы в этой модели. В случае возникновения инцидента с нелегитимным или подозрительным доступом система уведомляет офицера безопасности и выполняет действия по реагированию в зависимости от типа инцидента.

В основе решения находится шлюз доступа, который фиксирует и записывает сессии, проверяет права на те или иные действия каждой привилегированной учетной записи. Также реализовано управление паролями и секретами, чтобы минимизировать утечки, соблюдать правила регулярной смены паролей и не передавать лишнюю информацию за периметр. Система отказоустойчива и катастрофоустойчива, предусмотрено построение георазпределенных кластеров.

Наше решение СКДПУ НТ – это комплексная платформа контроля и мониторинга удаленных пользователей и доступов, как привилегированных, так и обычных.

Шлюз доступа дополняет система мониторинга и аналитики, которая помогает анализировать события. Этот продукт появился как решение проблем многих наших заказчиков, когда в высоконагруженных системах специалисту или даже команде специалистов ИБ трудно идентифицировать, что является инцидентом, а что нет. Современный PAM фиксирует не только видеозапись или клавиатурный ввод, но и запуск-остановку процессов, текстовый и файловый буфер обмена, блокирует часть подпротоколов при работе с RDP и SSH. То есть появилась необходимость в инструменте, который проводил бы максимально быстрый анализ с возможностью не только идентифицировать отклонения в поведении пользователей и хостов, но и реагировать на них.

Сейчас функционал системы мониторинга и аналитики позволяет обеспечить анализ более одного шлюза доступа в инфраструктуре: предоставить отчеты, сформировать поведенческие модели, детектировать аномалии и среагировать на них в рамках контура. Таким образом выстраивается дополнительный эшелонированный барьер от несанкционированного доступа и утечек информации.

В экосистему СКДПУ НТ входит портал доступа – удобный пользовательский интерфейс с настроенными политиками доступных шлюзов, а также программно-аппаратный комплекс «Компакт».

Компания «АйТи Бастион» обеспечивает разработку, техническую поддержку, развитие и сертификацию решения в соответствии с требованиями регуляторов: СКДПУ НТ внесен в реестр отечественного ПО Минкомсвязи РФ; сертифицирован ФСТЭК России на соответствие требованиям РД НДВ-4; имеет сертификат соответствия требованиям РД НДВ-2 Минобороны РФ.

– Решение для контроля и безопасности привилегированного доступа в последнее время включил в свой портфель «РТК-Солар», другие российские вендоры тоже развивают PAM-направление. Насколько уверенно «АйТи Бастион» себя чувствует на конкурентном рынке, и на чем эта уверенность базируется?

– Монопольное положение – плохо для компании, без конкуренции снижаются требования к самим себе, а это неминуемо влияет на качество продукта. Поэтому мы можем только приветствовать развитие рынка систем безопасности привилегированного доступа и появления решений от лучших

отечественных разработчиков. Конкуренция держит в тонусе, заставляет постоянно проводить аудит собственного видения рынка, потребностей заказчиков и технологических возможностей. В результате выигрывает вся отрасль информационной безопасности, игроки движутся вперед и не могут себе позволить остановиться в развитии, иначе заказчики выберут другого вендора.

Наша уверенность как лидера сегмента PAM строится на технологических преимуществах продуктов СКДПУ НТ, гибкости интеграций с решениями самых разных разработчиков, отмеченной многими заказчиками работе техподдержки и удобством приобретения – благодаря разветвленной сети партнеров по всей России.

– У вас много дистрибьюторов и партнеров-интеграторов, а как обстоят дела с технологическими коллаборациями? С кем и как вы работаете, что это дает заказчику?

– Мы всегда ищем новые возможности для технологического партнерства, на сегодняшний момент реализовали совместные проекты с 30 российскими компаниями в области ИБ. В частности, с «Лабораторией Касперского» у «АйТи Бастион» есть не только продуктовая интеграция СКДПУ НТ и Kaspersky Industrial CyberSecurity (KICS), но и соглашение по использованию наработок обеих компаний для создания безопасной системы доступа пользователей к промышленному сегменту сети предприятия, полному контролю их действий в периметре.

Одна из недавних интеграций – с компанией «Газинформсервис». Ее систему Ankey SIEM NG теперь можно использовать совместно с СКДПУ НТ, что повышает уровень кибербезопасности предприятия и позволяет эффективно реагировать на инциденты в режиме реального времени.

Зачастую, готовя новые коллаборации, мы отталкиваемся от запросов заказчиков. Новых запросов много, потому что рынку нужно решать вопросы импортозамещения, соблюдения меняющихся регламентов, внедрения принципиально новых технологий в корпоративные процессы.

– Расскажите подробнее о недавно представленном обновленном продукте «Синоникс». Зачем рынку такой шлюз безопасности?

– «Синоникс» – это цифровой шлюз безопасной передачи данных между изолированными сетями. Устройство позволяет организовать безопасный обмен информацией между узлами одной сети или разными сетями, предотвращая распространение киберугроз и вредоносного взаимодействия между ними. Принцип работы заключается в изолировании сетей, когда две сети, объединенные через «Синоникс», становятся невидимыми друг для друга. Благодаря встроенной технологии изоляции и передачи пакетов нейтрализуются сетевые атаки на 1–4 уровнях семиуровневой модели OSI. Синоникс ограничивает количество систем, которые могут получить доступ к сторонним продуктам, а также проверяет наличие корректного сертификата для передачи файлов между сетями.

Фактически мы решаем задачу синхронизации не только двух сетей, но и двух организационных структур внутри компании за счет того, что разрешения на передачу должны быть одобрены двумя «живыми» людьми, которые ответственны каждый за свою сеть. Для реализации этой концепции предусмотрена дополнительная блокировка устройства двумя специальными «пусковыми» ключами.

С помощью «Синоникса» удалось решить конкретные бизнес-задачи наших заказчиков при объединении сетей и их сегментов, когда необходимо минимизировать риски, при этом обеспечить эффективность и непрерывность обмена данными и файлами.

В прошлом году решение «Синоникс» получило новую платформу и стало на 100% импортозамещенным. Кроме того, обновленный шлюз может использоваться в сочетании с PAM-системой СКДПУ НТ, обеспечивая не только высокий уровень контроля проходящей между сетями информации, фильтрации и защиту от атак на транспортном уровне, но и управление привилегированным доступом внутри закрытого сегмента.

– Ваш прогноз на ближайшую перспективу: каким будет ландшафт угроз в промышленной и не только информационной безопасности?

– Объекты КИИ продолжат оставаться приоритетной целью для квалифицированных хакеров, и российским операторам систем управления значимыми объектами предстоит столкнуться с новыми вызовами ИБ. Исследователи трендов кибербезопасности в один голос говорят о том, что доля целевых атак неуклонно растет, и тренд продолжится. Одновременно целевые атаки становятся «комплексными» – с использованием двойного вымогательства, когда выкуп требуют и от скомпрометированной организации, и от ее клиентов. Или же от скомпрометированного подрядчика и от заказчика.

Введение оборотных штрафов смещает фокус атак: красть персональные и конфиденциальные данные станет сложнее и, как следствие, вырастет число взломов ИТ-инфраструктур с целью «вырубить» базовые сервисы. Очевидная мишень – дата-центры и операторы связи. Масштаб возможного ущерба трудно переоценить, это удар одновременно и финансовый, и репутационный.

Что касается сферы разработки СЗИ, то импортозамещение будет сильным драйвером для производителей. В АСУ ТП большинство компаний проводит импортозамещение с учетом требований по кибербезопасности, поэтому приходится пересматривать весь ИТ-ландшафт и применяемые технические средства. На стадии проектирования появляются идеи об использовании технологически сильных продуктов для решения новых задач. Это отличная среда для возникновения технологических альянсов. ■