

Сергей БОЧКАРЁВ:

«Наша компания была готова к росту количества проектов»



– Как события прошедшего года повлияли на развитие вашего бизнеса?

– В начале 2022 г. значительно возрос интерес к нашему продукту СКДПУ НТ. Для некоторых заказчиков это было вызвано острой необходимостью, другие

Промышленные объекты остаются мишенью для атак злоумышленников. Важность организации контролируемого доступа к АСУ ТП понимают на предприятиях различных отраслей. Об основных тенденциях в сегменте контроля привилегированных пользователей, направлениях развития продуктов и роли мер господдержки участников ИТ-рынка рассказал генеральный директор ООО «АйТи Бастион» Сергей Бочкарёв.

увеличился более чем в два раза. Наша компания была готова к росту количества проектов. Зрелость решения СКДПУ НТ позволила удовлетворить требования заказчиков.

– Какие проекты в промышленности оказались наиболее интересными?

– Интересно то, что количество проектов в промышленном сегменте за 2022-й выросло в два раза по сравнению с предыдущим годом. Наибольшее число пилотов также состоялось на сетях промышленных предприятий. Это красноречиво говорит о том, что в промышленности понимают важность организации контролируемого доступа к АСУ ТП.

телекоме. Госсектор и нефтегазовый были и остаются драйверами импортозамещения.

– В каком направлении развивается рынок контроля привилегированных пользователей в России и мире? Как вы оцениваете коллаборацию с другими рынками, такими как антивирусный или инструментов контроля защищенности?

– Контроль привилегированных пользователей развивается сразу в нескольких направлениях. С одной стороны, производители – и мы в том числе – наращивают функциональность продуктов. Например, наш комплекс СКДПУ НТ не только управляет доступом, но и предоставляет возможности поведенческого анализа, мониторинга и централизованного поиска, настраиваемой отчетности.

С другой стороны, уже не первый год мы идем по пути технологических интеграций с лидерами рынка, производящими соседствующие с нами ИБ-решения. За прошлый год мы подтвердили технологическую совместимость СКДПУ НТ с решениями компаний «СайберЛимфа», «Доктор Веб», «С-Терра СиЭсПи», «Газинформсервис», «Аладдин» и др.

– Насколько повлияли на рынок промышленной ИБ меры поддержки

Зрелость решения СКДПУ НТ позволила удовлетворить требования заказчиков.

просто поняли, что доступ нужно контролировать и стали смотреть «в сторону ПАМ». Мы оперативно нарастили число специалистов, усилили техподдержку – в целом за год штат «АйТи Бастион»

Однако хочу сказать, что значительно увеличилось количество проектов не только в промышленности, но и в других отраслях – в государственном секторе, нефтегазовом,

отечественных производителей, которые были предложены правительством в прошедшем году?

– Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» повлиял на рынок несомненно. Повысилась персональная ответственность владельцев бизнеса за допущение и устранение последствий инцидентов информационной безопасности. Стало понятно, что от кибербезопасности не отмахнуться, необходим анализ угроз для конкретного предприятия. Думаю, что выполнение требований указа повысит

реальную безопасность в России, и не только бумажную, а также поддержит отечественных производителей в сфере информационной безопасности.

Не могу не отметить работу Министерства цифрового развития, связи и массовых коммуникаций РФ в 2022 г. Благодаря поддержке правительства мы смогли сохранить и нарастить команду, не потеряли ни одного важного специалиста. Мы видим, что для Минцифры действительно важно сохранить и поддержать отрасль, за что мы благодарны.

– Какие события на рынке промышленного ИБ вы ожидаете в 2023 году?

– Последние лет пять промышленность входит в пятерку отраслей, наиболее активно атакуемых злоумышленниками. Не думаю, что что-то изменится в текущем году. Промышленные объекты остаются мишенью для атак, доступы в дарквебе будут продаваться еще активнее. Это означает, что нам как разработчикам системы контроля доступа нужно будет развиваться и дальше.

Интересные кейсы, связанные с АСУ ТП, у компании «АйТи Бастион» уже есть. О некоторых из них мы расскажем на нашем круглом столе в рамках форума 15 марта, а также готовы тет-а-тет делиться информацией на нашем стенде. ■

«АйТи Бастион» объявляет о выходе нового релиза комплекса СКДПУ НТ

В обновленной версии 2.2.8 добавлено несколько принципиально важных для заказчиков функциональных возможностей.

Теперь пользователям доступен новый модуль СКДПУ НТ Портал доступа – сервис, который предоставляет возможность централизованного доступа через единый веб-интерфейс к целевым системам, подключенным к разным шлюзам доступа СКДПУ НТ. Портал доступа объединяет в виде списка все разрешенные политической доступа ресурсы. Он упрощает работу с системой для самих привилегированных пользователей, позволяя им быстро находить нужные доступы в веб-интерфейсе. Все доступы теперь под рукой, объединены вместе, и их можно группировать по типу устройств, площадке или по личным предпочтениям.

Кроме того, в новой версии СКДПУ НТ появилась возможность подключения дополнительных внешних сервисов обогащения данных. Теперь пользователь может в несколько действий подключить системы сторонних производителей для выполнения контроля обхода средств защиты, что особенно важно для объектов КИИ. Реализована технологическая интеграция с KICS от «Лаборатории Касперского», PT ISIM от Positive Technologies, ARMA производства компании InfoWatch и DATAPK от компании CyberLympha.

Также в системе контроля привилегированного доступа СКДПУ НТ версии 2.2.8 расширен уже существующий функционал продукта. Так, новый механизм анализа эффективности сессий одновременно работает

с текущими сессиями и историческими данными. Теперь решение накапливает информацию по конкретному администратору и сигнализирует о резком сокращении или превышении времени его работы на инфраструктуре. Собранные данные отражаются в отчете об эффективности сессии.

В новой версии улучшены анализаторы потенциально опасных команд, отчеты предоставления данных, пользовательский интерфейс стал более удобным, а также реализованы другие улучшения текущего функционала. Также в данной версии реализован ряд архитектурных улучшений и устранены предыдущие ошибки в продукте.

«В новой версии СКДПУ НТ мы бы хотели обратить отдельное внимание заказчиков на Портал доступа. Это новый продукт, который в разы повысит удобство работы специалиста на больших инфраструктурах с большим числом шлюзов и одновременных сессий. В первую очередь он нацелен на улучшение пользовательского взаимодействия с системой и делает работу с ней эффективнее и проще. Также стороной не обошли и вопросы улучшения качества собираемых и обрабатываемых данных в системе. Речь не только об интеграциях с промышленными системами обнаружения вторжений типа KICS, PT ISIM, IW ARMA и DATAPK, их совместная работа подтверждена и эффективна, но и об анализе эффективности работы пользователей, основанном на данных, полученных из сессий», – комментирует технический директор **Дмитрий Михеев**.