Справка о компании

ООО «АйТи Бастион» - российский разработчик систем контроля привилегированного доступа СКДПУ НТ и шлюза безопасной передачи данных и файлов между изолированными сетями «Синоникс». В Республике Беларусь решение СКДПУ НТ входит в реестр СЗИ, прошедших сертификацию ОАЦ (рег. номер сертификата соответствия BY/112 02.02. ТР027 036.01 00571).

В портфеле «АйТи Бастион» свыше 250 реализованных проектов, более 300 партнеров-интеграторов в РФ и РБ, реализовано 30 технологических коллабораций с ведущими российскими вендорами. Среди заказчиков — государственные структуры, ведущие компании финансового сектора, энергетической отрасли, промышленности, ритейла, логистики, сельского хозяйства и др.

«АйТи Бастион» работает на рынке технологий кибербезопасности с 2014 года, главный офис находится в Москве.

На вопросы организаторов IT-SECURITY CONFERENCE о потребностях и ожиданиях заказчиков на нашем рынке ответил руководитель технического центра «АйТи Бастион» Владимир Алтухов.

- Какие сейчас самые актуальные проблемы, с которыми сталкиваются крупные организации, оперирующие критически значимыми данными?

- В Республике Беларусь, как и в России, сейчас остро стоит вопрос миграции с зарубежных решений информационной безопасности. Это непростой процесс, требующий средств, экспертизы и определенной зрелости в принятии решений об управлении ИТ-инфраструктурой. На фоне продолжающегося уже не первый год роста кибератак на информационное пространство России и Беларуси использование привычных продуктов иностранных вендоров – без обновлений или полноценной технической поддержки – не только является раздражителем для регуляторов, но и ставит под удар комплексную безопасность предприятия. При этом у крупных заказчиков, которые быстрее закрывают потребности своих ИТ- и ИБ-служб, появилась еще одна проблема: их подрядчики, не имеющие полноценного арсенала средств защиты информации, становятся источником угрозы. Ведь с точки зрения злоумышленника рациональнее атаковать именно незащищенные цепочки поставок, а не пытаться взломать эшелонированную систему целевого объекта.

- То есть чтобы нивелировать риски кибербезопасности, всем субъектам той или иной отрасли нужно по максимуму оснащаться средствами информационной защиты всех классов?

- Вряд ли такая ситуация достижима, поскольку всем нужны разные СЗИ под разные задачи и бюджеты, к тому же в природе не существует столько специалистов ИБ для обслуживания такого количества систем. Ответственный подход здесь должен формироваться со стороны критически важных для экономики организаций – обеспечить целостность данных внутри инфраструктуры является их первоочередной обязанностью. Причем все должны понимать, что угроза компрометации необязательно исходит извне, собственный персонал в половине случаев становится источником инцидентов информационной безопасности.

Для решения таких задач мы предлагаем линейку продуктов защиты привилегированного доступа СКДПУ НТ. Данная система контролирует, записывает, формирует поведенческую модель и по необходимости

принудительно прерывает действия администраторов и других привилегированных пользователей, у кого есть доступ к важным ресурсам инфраструктуры, – это внутренний персонал, внешние аудиторы, пентестеры, поставщики ИТ-услуг и другие подрядчики.

Когда ИБ-служба знает, кто, что и когда делал в системе, ей значительно легче расследовать инциденты, не допускать их повторения и обучать персонал.

- Какая отрасль сейчас испытывает наибольшее давление – со стороны организованных хакерских группировок и регулирующих органов, требующих соответствия жестким регламентам ИБ?

- Традиционно это все организации с критически важной ИТ-инфраструктурой, в Республике Беларусь таковых около 300. Отдельно я бы выделили банковско-финансовый сектор, где рост активности злоумышленников наиболее заметен: МВД Беларуси за неполный 2023 год фиксировало более 10 тыс. преступлений в финансовом секторе, что вдвое больше показателей 2022 года. Причем не о всех атаках становится известно, поэтому реальные цифры по инцидентам кибербезопасности традиционно больше. При этом для банковской отрасли характерны все те же угрозы, что и для предприятий промышленности, энергетики, торговли, государственных ведомств:

- действия злоумышленников, в том числе несанкционированные соединения с системами процессинга и приложениями;

- ошибочные или намеренно деструктивные действия администраторов подрядчиков;

- случайные ошибки сотрудников банка или их злонамеренные поступки при работе в периметре инфраструктуры.

От всех перечисленных угроз надежно защищают системы PAM (Privileged Access Management). Наш продукт данного класса СКДПУ НТ соответствует требованиям Технического регламента Республики Беларусь и может применяться на значимых объектах.

- Защита доступа – не единственная специализация «АйТи Бастион». Расскажите об обновленном продукте «Синоникс», который вы привезли в Минск.

- «Синоникс» – это шлюз безопасного объединения изолированных сетей или их сегментов. Устройство позволяет организовать безопасный обмен данными и файлами между узлами одной сети или разными сетями, предотвращая вредоносное взаимодействия между ними и распространение киберугроз. 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.

Также мы решили 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» уже удалось закрыть конкретные бизнес-задачи наших заказчиков при объединении сетей и их сегментов – когда необходимо минимизировать риски, обеспечив эффективность и непрерывность обмена данными и файлами.

В прошлом году «Синоникс» оснастили новой платформой, и теперь он на 100% импортозамещенный. Кроме того, обновленный шлюз может использоваться в сочетании с PAM-системой СКДПУ НТ. Так заказчик обеспечивает 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.