В поисках аномалий, или Как избежать утечек из-за «человеческого фактора»

Комплексный продукт СКДПУ НТ компании «АйТи БАСТИОН» позволяет защитить доступ к инфраструктуре организации и увидеть, какие действия на ней выполняют собственные сотрудники, подрядчики и аудиторы. О том, чем СКДПУ НТ полезен банкам, рассказывает технический директор «АйТи БАСТИОН» Дмитрий Михеев

Текст
АЛЕКСАНДРА НИКОЛЬСКАЯ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Дмитрий, кредитные и страховые организации составляют значительную часть заказчиков «АйТи БАСТИОН». Почему именно они?
— Финансовые организации традиционно внимательны к анализу рисков. Они же эксплуатируют сложные информационные системы, в том числе в разных режимах аутсорса и удаленного доступа, и логично, что риски такого доступа они контролируют. Это как раз профиль нашего продукта, поэтому в банковском секторе он востребован.

— Какая именно аналитика, предоставляемая системой, наиболее востребована в таких организациях?
— В зависимости от параметров системы это могут быть отчеты о ресурсах, нагрузке на систему и компоненты инфраструктуры, в первую очередь в пользу IT-отдела. Это также отчеты, связанные с работой нашей подсистемы анализа аномалий и контроля поведения пользователей — например, отчеты о движении данных или о значительном изменении состава действий, выполняемых пользователем. Далеко не всегда это инцидент, но ситуация такова, что заказчикам необходимо обычно скромными силами контролировать масштабные и критически важные системы. Чтобы увидеть все происходящие события, не хватает физических ресурсов, поэтому в рамках нашего продукта решается задача «подсветить» для операторов ИБ наиболее «интересные» для них ситуации — потенциально опасные «в моменте» или в развитии.

— Чем продукт СКДПУ НТ может быть еще полезен банкам и каким их подразделениям?
— Мы можем быть интересны как отделам, занимающимся эксплуатацией средств доступа, так и ответственным за информационную безопасность. За счет анализа аномалий наш продукт позволяет меньшими силами контролировать более крупные системы, это основной профит для заказчиков.

Продукт позволяет накапливать историю изменений, вносимых пользователями, поэтому можно как реагировать на развивающиеся сценарии, так и производить подробные разборы полетов, при необходимости — на «большую глубину». В частности — отвечать на вопросы, что происходило с данным сервером в данный период или кто из администраторов заслуживает большего внимания и почему.

— Есть ли у компании видение, что нужно ИБ-подразделениям банков в настоящее время?
— Мы стараемся собирать интересные сценарии от всех заказчиков. Каждое общение с потенциальными или существующими заказчиками привносит в копилку идеи, которые мы стараемся реализовывать как подходы или функции внутри системы.

У ИБ-подразделений банков есть особенности — пристальное внимание регуляторов, много очевидных практических рисков под контролем, высокий уровень ответственности, масса используемых средств защиты, а также значительные масштабы защищаемых инфраструктур. При этом даже у очень крупных организаций работы гораздо больше, чем имеющихся человеческих ресурсов. Отсюда возникают пожелания, например, к гранулярности настройки функциональных модулей, а также к достаточно изощренным отчетам. Б.О