Как контролировать доступы к виртуальным средам, когда администраторами стали все

Использование средств виртуализации ресурсов пользователей (VDI) — активно набирающий популярность подход для обеспечения удобства и эффективности работы организаций любого масштаба. В особенности это характерно для кредитных организаций: во-первых, потому что в их инфраструктуре традиционно работает сразу несколько команд — и собственных, и привлеченных; во-вторых, по причине удобства изоляции внутренних ресурсов компании в закрытом виртуальном пространстве; в-третьих, потому что это сильно упрощает процесс обслуживания и администрирования рабочих мест пользователей

Текст
КОНСТАНТИН РОДИН,
РУКОВОДИТЕЛЬ ОТДЕЛА РАЗВИТИЯ ПРОДУКТОВ «АЙТИ БАСТИОН»



С уходом иностранных решений приходится пересматривать привычные механизмы управления виртуальными средами, к тому же сам по себе процесс импортозамещения весьма непростой и оказывает значительную нагрузку на IT- и ИБ-службы. При этом потребность в VDI растет вместе с вниманием регуляторов к обеспечению конфиденциальности данных.

Я не просто так отметил нагрузку, навалившуюся на тех, кто отвечает за работоспособность информационной инфраструктуры. Ведь она в том числе формируется, когда IT-службы постоянно просят предоставить им доступ для работы с виртуальными машинами, а ИБ-службы тратят время на проверку и предоставление прав. В итоге мы получаем отчасти патовую ситуацию: IT старается внедрить удобные средства управления и предоставления рабочих мест, а службы ИБ стараются уследить не только за реальными нарушениями безопасности, но и за потенциальными.

Совершенствуя свой продукт СКДПУ НТ для контроля и управления привилегированным доступом, компания «АйТи Бастион» разработала решение, позволяющее автоматизировать предоставление доступа к виртуальным ресурсам пользователей финансовой организации, и при этом привнести в него новые уровни безопасности, которые ранее были характерны только при контроле привилегированного доступа к IT-инфраструктуре. Механизм реализован в концепции единого окна с функциями контроля, мониторинга и поведенческого анализа действий пользователей.

От контроля администраторов к контролю каждого пользователя

Ключевые показатели безопасности инфраструктур рабочих столов и других ресурсов в виртуальной среде финансово-кредитной организации требуют полноценного контроля доступа:

- записи в формате видео и текста действий сотрудников;
- защиты удаленного доступа с возможностью детального анализа событий и детектирования отклонений поведения;
- удобства администрирования при автоматизации добавления ресурсов и управления ими в системе виртуализации;
- удобства эксплуатации — речь идет об уже реализованной совместимости платформы СКДПУ НТ с ведущими российскими разработчиками систем виртуализации и других IT- и ИБ-решений.

Концепция единого окна реализована с применением универсального интерфейса. В нем создается запрос под пользовательской учетной записью на создание или удаление ресурсов в доступном виртуальном простран-

стве. На каком бы устройстве ни работал пользователь, система проанализирует его права и предоставит или не предоставит ресурсы, доступ к которым осуществляется согласно политикам безопасности. При этом информация об изменениях в рамках политик доступа после привязки ресурса к пользователю автоматически передается на сервер СКДПУ НТ. В дальнейшем такие учетные записи и связанные с ними целевые устройства остаются под полным контролем PAM-платформы.

Десятилетний опыт компании «АйТи Бастион» показывает, что функции СКДПУ НТ нужны не только «безопасникам», но и бэк-офису для накопления доказательной базы, а еще для бизнес-аналитики, особенно когда события необходимо анализировать в оперативном режиме.

Разрабатывая решения по автоматизации контроля доступа в VDI, мы в первую очередь ориентировались на IT-отделы, при этом учитывая требования служб ИБ. Это путь автоматизации не столько решений, сколько бизнес-процессов — связанных с ними задач по предоставлению, согласованию и отзыву доступов. Из цепочки исключаются многочисленные «ручные» согласования, а специалисты ИБ получают полный контроль над доступом без усложнения администрирования новых прав.

Операционный эффект от автоматизации и контроля доступа

- Пользователи получают оперативный доступ к ресурсам без дополнительных действий со стороны смежных отделов и в рамках единой системы подтверждения доступа.
- Снижается общая стоимость владения виртуальной инфраструктурой с дополнительными средствами контроля доступа за счет автоматизации процесса работы систем.
- Соблюдаются требуемые регламенты работы служб IT и ИБ в части эффективности, скорости и безопасности работы и в части соответствия требованиям по импортозамещению ПО.

Не доступом пользователей едины

Работая с аналитикой рисков утечки данных, разработчики «АйТи Бастион» выявили потребность сложных инфраструктур в обеспечении безопасности обмена данными и файлами между изолированными сетями. Для финансовых учреждений это могут быть обмен, отправка и получение данных с единого корпоративного сервера между ними и аудиторами или регуляторами. Процессы необходимые, но каждый раз требующие очень внимательной организации безопасного процесса передачи данных из одной инфраструктуры в другую.

Решение для предотвращения вредоносного взаимодействия между разными узлами при обмене файлами и данными получило название «Синоникс». Принцип работы шлюза безопасности заключается в том, что в процессе передачи две сети становятся невидимыми друг для друга.

Подробнее о сценариях применения «Синоникса», его технологических возможностях при изоляции и передаче информации представители «АйТи Бастион» расскажут в следующих обзорах, а также по запросу в индивидуальном порядке. Б.О



Реклама