С единым паролем

«ТрансТелеКом» стала первой отечественной компанией, внедрившей решение по управлению учетными записями пользователей IBM Tivoli Identity Manager

О продукте IBM Tivoli Identity Manager компания «ТрансТелеКом» узнала в конце 2004 года на семинаре, проводившемся компанией «Открытые Технологии». В одной из презентаций рассказывалось о технологии однократной регистрации для портальной среды. Реализация данного решения в числе прочего предполагала использование продукта IBM Tivoli Identity Manager.

Компания решилась на серьезный инфраструктурный проект по централизации управления учетными данными. Однако для бизнеса основная ожидаемая ценность заключалась в однократной регистрации пользователей. Бюджетный комитет компании принял решение о реализации проекта именно с этой целью. Тем не менее когда распоряжение о проведении проекта получила служба информационной безопасности, в ней прекрасно поняли, что получат все преимущества, связанные с централизацией управления: единый процесс заведения учетных записей и учета их жизненного цикла, предоставления и аудита выданных прав. Все эти факторы являются важными для любого департамента безопасности.

Требование безопасности

В компании «ТрансТелеКом» разработано большое количество приложений на базе IBM Lotus Notes по продаже услуг и их учету. Усилиями собственных разработчиков создано 15 баз данных только в центральном отделении. У каждой системы существует свой интерфейс, свои требования к администраторам, свои настройки безопасности. Нельзя сказать, что процесс предоставления доступа к ним не был автоматизирован вовсе. «Тем не менее разработанные процедуры фактически не работали: активно практиковалась выдача прав согласно индивидуальным договоренностям в обход политик безопасности», — отметил начальник отдела информационной безопасности компании «ТрансТелеКом» Дмитрий Соболев.

Ориентация на запросы пользователей — неверная стратегия с точки зрения безопасности. В этом случае каждый менеджер может потребовать у администратора получение доступа к той или иной системе, что приводит к возникновению огромного количества неструктурированных полномочий, в итоге отдел информационной безопасности теряет контроль над соответствием прав доступа принятой политике. Вполне естественно, что при этом не ведется никакой документации, и у многих пользователей образуется уникальный набор привилегий.

Таким образом, можно сказать, что ситуация для внедрения IBM Tivoli Identity Manager была идеальная. Среди поставленных перед проектом задач можно выделить централизованное управление паролями (была нужна единая политика — самая сложная из всех возможных, с длиной и сроком использования паролей), создание и автоматизацию единого процесса по предоставлению доступа, а также возможность получения отчетов о процедурах предоставления доступа. Но в качестве главного видимого эффекта выступал механизм однократной регистрации пользователей (Single Sign-On). Именно эта возможность обеспечила лояльность руководства компании и необходимую поддержку проекта с его стороны.

Система IBM Tivoli Identity Manager являлась наиболее работоспособным на тот момент решением, обеспечивающим управление учетными записями (на данный момент спектр предлагаемых на рынке решений несколько расширился). Помимо этого, система очень хорошо интегрируется с продуктами IBM Lotus, с которыми предстояло проводить основную часть работы по интеграции. Эти два фактора и определили окончательный выбор компании.

Два в одном

Система была относительно новой, по крайней мере, на отечественном рынке, что накладывало на проект дополнительные риски. Опыта по реализации этого решения не было, более того, не удалось найти информацию относительно зарубежного опыта внедрения IBM Tivoli Identity Manager в телекоммуникационных компаниях.

Еще одной проблемой стало серьезное сопротивление со стороны лиц, занимавшихся вопросами прав доступа: они почувствовали снижение своей ценности для компании. Надо сказать, что интересы служб внутренней автоматизации и безопасности несколько различались. Первая выступала против реализации проекта и считала, что никакое управляющее средство не заменит сертифицированного специалиста. Второй же надоели постоянные обходы политики безопасности, и она настаивала на внедрении жестких решений. Основное «непонимание» исходило именно со стороны ИТ-сотрудников (системных администраторов), что для ИТ-проекта является редким явлением. Проектной команде пришлось столкнуться с личными амбициями людей, не желающих оптимизировать свою деятельность.

Поскольку данных специалистов устраивала сложившаяся ситуация, то стандартная формулировка «меньше времени на рутину, больше времени на проекты» не работала. Зачастую вопрос приходилось решать силовыми методами. «Тем не менее первым средством, которое пытались применять, всегда была дипломатия», — подчеркнул Соболев.

Самым сложным было «убедить» все заинтересованные стороны в необходимости проекта. Если нет поддержки со стороны пользователей, такие масштабные проекты реализовать очень сложно. Тем не менее популярность проекта в среде высшего менеджмента сделала свое дело, и сопротивление было преодолено. Наиболее непримиримые администраторы были вынуждены покинуть компанию.

Кроме организационных проблем, были и технические. Система управления учетными записями и система однократной регистрации — это разные решения с различными подходами к реализации. Конечных пользователей, конечно же, интересует именно однократный ввод пароля. Вся сложность проекта заключалась в построении обеих систем.

Выстраивание собственно системы с единой точкой входа — нетривиальная задача. Однако при создании системы управления учетными записями все записи, существующие в компании, были сведены воедино, что значительно упростило решение: при наличии центрального хранилища записей и стандартных средств, предоставляемых объединяемыми решениями, создание однократной регистрации не должно представлять большой технической проблемы.

IBM Tivoli Identity Manager имеет множество коннекторов к системам других поставщиков, однако для некоторых из используемых «ТрансТелеКомом» решений их не существовало. Более того, внутренние разработки не учитывали потребности в интеграции. Ярким примером этого стала система технического учета и мониторинга — заказная разработка, выполненная внешним партнером. Эту проблему пришлось решать путем доработки соответствующего функционала решений.

Востребованная технология

Основная цель проекта была достигнута: пользователи получили единую систему паролей, а служба информационной безопасности — четкую и прозрачную политику доступа со стандартизованными процессами предоставления прав. При этом пользовательский интерфейс для изменения паролей было решено не реализовывать — это противоречило политике безопасности, которая в любой крупной компании является довольно жесткой. Все действия с паролями пользователей возложены на службу поддержки. Тем не менее количество персонала, занимающегося проблемами доступа, удалось серьезно сократить за счет автоматизированной системы, которая взяла на себя эти функции.

Внедрение любого инфраструктурного решения влияет на последующие ИТ-проекты. Данный случай не стал исключением. Опыт интеграции используемых приложений позволил конкретизировать требования компании к внедряемым решениям в плане управления доступом. Теперь любая новая система рассматривается не только с точки зрения присутствия необходимого функционала, но и на предмет наличия необходимых коннекторов.

«Ощутимая польза заключается в сокращении сроков реализации последующих проектов», — считает Соболев. Во-первых, значительно ускоряется вопрос согласования внедрения системы со службой информационной безопасности. Во-вторых, временные затраты на начальное администрирование системы и введение пользователей стали минимальными. Кроме того, удалось снизить издержки на сопровождение систем. Качество же получаемых ИТ-услуг повысилось за счет снижения человеческого фактора в процессе управления правами доступа.

В настоящий момент идет расширение использования IBM Tivoli Identity Manager: для систем, не охваченных этим решением ранее, дорабатываются коннекторы, и они подключаются к системе, обеспечивающей однократную регистрацию. Это важнейший показатель востребованности используемой технологии для организации.

IBM