IBM Tivoli на страже ИТ-безопасности

В основу системы информационной безопасности компании «ВымпелКом» положено решение IBM Tivoli Identity Manager

Компания «ВымпелКом» знакома в России очень многим пользователям мобильной связи. И немудрено: сети Beeline покрывают 11 временных зон страны. Желтый в черную полоску логотип неизменно вызывает хорошее настроение и желание последовать призыву: «Живи на яркой стороне!»

Вся эта яркость и праздник обеспечиваются усилиями сотрудников компании, число которых по всей России, где расположены более 100 региональных отделений, составляет около 14 тыс. человек. Но как бы ни был велик коллектив, его работа во многом основана на бесперебойном функционировании внушительной ИТ-инфраструктуры.

Несколько лет назад в компании «ВымпелКом» разработали и приняли к исполнению стратегию централизованного развития информационных технологий. «Это было непростое решение, потому что так вот причесать года три-четыре назад все под одну гребенку было очень сложно», — вспоминает Дмитрий Устюжанин, начальник отдела информационной безопасности «ВымпелКома». Однако, несмотря на постоянный экстенсивный рост компании и большое количество эксплуатируемых систем, сделать задуманное удалось, и «ВымпелКом» стал чуть ли не единственной компанией такого масштаба, которая смогла создать у себя централизованную ИТ-инфраструктуру. «Многие удивляются, как сегодня совсем небольшому количеству сотрудников удается управлять нашей ИТ-инфраструктурой, демонстрируя при этом хорошие показатели и позволяя с положительным результатом проходить аудиторские проверки», — отметил Устюжанин.

Аудит

Аудиторскую проверку на соответствие требованиям закона Sarbannes Oxley Act (SOX) компания прошла пока единожды. Такую проверку проходят все организации, которые размещают свои акции на Нью-Йоркской фондовой бирже.

ДМИТРИЙ УСТЮЖАНИН: «Создание системы управления идентификацией важно не только с точки зрения котировки акций «ВымпелКома» на Нью-Йоркской фондовой бирже. Основная задача, которая была решена в ходе реализации проекта, — это достижение уверенности компании в своей информационной безопасности»

Для справки: требования SOX направлены на упорядочение работы финансовых служб, прозрачность финансовой отчетности и обеспечение внутреннего контроля над всеми этапами и процессами ее формирования. Чтобы соответствовать требованиям этого закона, компании должны внедрять современные формы документооборота и перестраивать системы управления. Современный подход к управлению производственными процессами включает внедрение систем для автоматизации финансовой отчетности, проведения транзакций и составления отчетов для соответствующих органов внутреннего контроля.

Системы автоматизации в «ВымпелКоме» применяются достаточно широко, более того, вся деятельность компании зависит от информационных технологий. Именно в информационных системах осуществляется планирование и формируется отчетность, с этими системами работает подавляющее большинство сотрудников. В таких условиях необходимо было определить и реализовать ряд базовых требований к информационным системам.

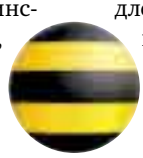
Четкая и прозрачная организация процесса управления доступом к информационным ресурсам — один из критериев соответствия закону Сарбейнса — Оксли. Очевидно, что с учетом масштабов компании и числа ее сотрудников управлять вручную матрицей доступа просто нереально. Поэтому в компании была создана специализированная система, точнее, сформированы процессы предоставления и контроля доступа, а также составления соответствующих отчетов по этим процессам.

Эта специализированная система создавалась около трех лет. В ее основу были положены продукты IBM Tivoli. Партнером в данном проекте выступила компания CompuTel — системный интегратор, работающий на рынке ИТ с начала 1994 года. CompuTel специализируется на разработке комплексных интегрированных решений для создания надежно работающей ИТ-инфраструктуры предприятия с учетом индивидуальных потребностей заказчика.

Работа была проделана огромная. Только на формулировку требований к будущей системе ушло около полугода. К этому процессу были привлечены несколько подразделений компании «ВымпелКом». В ходе внедрения, по словам представите-

лей CompuTel, процесс обучения, производившийся поначалу в сертифицированном IBM учебном центре CompuTel, был дополнен специально разработанными курсами, которые читались на территории заказчика.

«Закон SOX не требует внедрения какой-то конкретной автоматизированной системы, — разъяснил Устюжанин. — Необходимо обеспечение определенного уровня контроля ИТ-инфраструктуры. При помощи каких средств это будет реализовано, каждая конкретная организация решает самостоятельно. Единственное требование состоит в том, что аудиторам нужно предъявить доказательства, что такой контроль в компании осуществляется, и продемонстрировать, как это работает».



Билайн™

Аудит на соответствие закону Сарбейнса — Оксли — ежегодный процесс. «Чтобы аудиторы дали положительное заключение, организация должна постоянно находиться в тонусе и демонстрировать это», — отметил Устюжанин.

ИТ-безопасность

Тема информационной безопасности в последние годы все более смещается от вопросов, связанных с внедрением конкретных систем (антивирусов, межсетевых экранов и др.), к общей проблеме организации процесса. Основная задача информационной безопасности — четко понимать, что происходит при взаимодействии пользователей с информационными системами, кто и к каким приложениям имеет доступ, как реализуются возможности построения отчетов, проведения анализа деятельности и т. д.

Практика показывает, что риски, связанные с использованием информационных технологий, в основном внутренние, присущи как самим информационным системам, так и организации, использующей их в своей работе. Поэтому одним из важных архитектурных компонентов ИТ-безопасности компании «ВымпелКом» является процесс управления идентификацией (Identity Management), помогающий организовать систему доступа к ИТ-ресурсам и проконтролировать правильность ее работы. Процесс организован на основе решений IBM Tivoli, а также IBM WebSphere.

Продукт IBM Tivoli Identity Manager используется как централизованный инструмент для управления учетными записями пользователей в различных инфраструктурных и бизнес-системах заказчика. Данный модуль является ядром системы и позволяет централизованно выполнять все действия по управлению жизненным циклом учетной записи пользователя приложения (создание, удаление, блокировки, изменение атрибутов и принадлежности к группам, смена пароля), причем оператору не нужно знать специфики управляемых приложений и даже иметь к ним административный доступ.

IBM Tivoli Identity Manager интегрируется с кадровыми системами и позволяет соотнести конкретного человека и его сеансы доступа во все системы, что открывает большие возможности для аудита различных аспектов ИТ-безопасности (например, можно легко выявлять уволенных сотрудников, у которых не заблокирован доступ).

Продукт IBM Tivoli Directory Integrator позволяет гибко объединять данные, расположенные в различных каталогах и базах данных. В этом проекте он использовался для обеспечения связи IBM Tivoli Identity Manager с системами разработки заказчика, для которых в данном продукте нет собственных интерфейсов.

Решения IBM WebSphere обеспечили в проекте сервер приложений для различных подсистем управления идентификацией, а также унифицированный пользовательский интерфейс для доступа операторов и администраторов к системе.

ИТ-безопасность — важнейшая характеристика качества бизнеса сотового оператора, работающего на высококонкурентном рынке

В компании «ВымпелКом» в ходе реализации процесса предоставления и контроля доступа был определен весь комплекс контрольных процедур. Однако, по словам Устюжанина, принципы безопасности — ответственность, четкий подход, понимание, что и как нужно выполнять, — необходимо было внедрить во все бизнес-процессы. Сегодня все это уже стало частью повседневных служебных обязанностей. «Перестройка произошла внутренняя, в головах наших сотрудников», — отметил Устюжанин.

ИТ-безопасность — важнейшая характеристика качества бизнеса сотового оператора, работающего на высококонкурентном рынке. Один из многих рисков в данной области — так называемый человеческий фактор. Неумелые действия персонала в одночасье могут привести к сбоям в системе. Вся бизнес-информация требует бережного обращения, но, в соответствии с законодательством РФ, не менее надежно нужно хранить большое количество персональных данных. Анализ рисков и внедрение необходимых мер защиты в различные компоненты ИТ-инфраструктуры, обеспечение непрерывности предоставления технологических сервисов, координация требований по безопасности во всех региональных отделениях и, наконец, соответствие закону Сарбейнса — Оксли и местному законодательству — все это составляет политику безопасности компании «ВымпелКом».

По словам Устюжанина, создание системы управления идентификацией важно не только с точки зрения котировки акций «ВымпелКома» на Нью-Йоркской фондовой бирже. Основная задача, которая была решена в ходе реализации проекта, — это достижение уверенности компании в своей информационной безопасности.

Результаты и планы

В компании «ВымпелКом» создана система управления идентификацией, которая охватывает основные инфраструктурные и бизнес-системы, а также сформирован централизованный справочник с информацией об актуальных сеансах доступа сотрудников к информационным системам.

В компании появилась возможность проводить автоматизированный аудит целевых систем на предмет соответствия требованиям информационной безопасности в части доступа пользователей к критичным информационным системам. Кроме того, в автоматическом режиме проводятся корректирующие воздействия на целевые системы при обнаружении несоответствия требованиям информационной безопасности. Это дает возможность мгновенно, частично или полностью блокировать доступ нарушителя к системе.

На повестке дня стоит вопрос организации взаимодействия и распространения отработанных принципов информационной безопасности на страны СНГ, с учетом требований местных законов в этой сфере. ✖