

Одним ударом — сразу девять зайцев.

Опыт внедрения LANDesk



текст: Андрей Шуклин

Необходима была система, позволяющая контролировать работу компьютерного парка всех офисов и подразделений в реальном времени: отслеживать состояние ПО, наличие обновлений, обеспечивать четкое разделение доступа, чтобы избежать риска утечки информации.

ПРОБЛЕМЫ ИНФРАСТРУКТУРЫ

До начала внедрения инфраструктура ГИБ представляла собой разрозненную

компьютерную среду, в рамках которой администратор каждого филиала вел свою политику. Дополнительные сложности для проведения инвентаризации и контроля инфраструктуры создавала сама система обслуживания техники и технической поддержки сотрудников. Отказавшись от непрофильных активов, банк передал обслуживание компьютерной сети на аутсорсинг сторонней компании, в результате чего значительно облегчилась поддержка пользователей и обслуживание компьютерного парка, но усложнился процесс контроля IT-составляющей бизнеса. Для выхода из ситуации было решено внедрить комплексное ПО, позволяющее контролировать и сводить всю информацию о компьютерном парке в одно «окно», доступное руководителям компании.

ВЫБОР РЕШЕНИЯ

При рассмотрении различных вариантов решения проблемы IT-специалисты банка остановили свой выбор на системе LANDesk Management Suite, главным аргументом в пользу которой стали мощь и гибкость в решении текущих задач по управлению компьютерным парком и технической поддержке конечных пользователей.

Вторичную, но не менее важную роль сыграли минимальные требования системы LANDesk Management Suite к IT-инфраструктуре. Для развертывания системы, управляющей сотнями и тысячами компьютерами во множестве удаленных филиалов достаточно одного сервера с минимальными характеристиками. При этом

осуществляется не только полнофункциональное управление компьютерным парком, но и обеспечивается минимизация нагрузки на каналы передачи данных.

После всех согласований и выполнения пилотного проекта началось непосредственно внедрение. Развертывание сервера LANDesk и установка агентов на ПК центрального офиса и филиалов ГИБ заняло несколько дней. Еще около двух недель понадобилось на наладку функционала и приемо-сдаточные испытания. Все работы были выполнены специалистами ARBYTE находясь в Москве.

«Распространение клиентов всегда происходит достаточно просто, — отметил менеджер проекта Владимир Максимов. — Минимальный размер файла, который необходимо записать на каждый компьютер, составляет около 300 Кбайт, которые легко передать за минуту по любому каналу связи. Единственная сложность состояла в том, что удаленный доступ к некоторым компьютерам был закрыт, и нам приходилось связываться с региональными администраторами и просить их открыть доступ по определенному порту».

АУДИТ И ИНВЕНТАРИЗАЦИЯ

Когда программные агенты LANDesk были распространены по всем компьютерам сети, система начала самостоятельно собирать информацию об их состоянии и актуальности установленного программного обеспечения.

Первое сканирование уязвимостей, проведенное после установки ПО LANDesk,

СПРАВКА

«Городской Ипотечный Банк» (ГИБ) — один из крупнейших специализированных банков России (собственный капитал около 1,9 млрд рублей), давший старт программе жилищного ипотечного кредитования в нашей стране, был основан в марте 2004 года. С его помощью более 10,5 тыс. российских семей решили самый насущный для многих из них вопрос — жилищный: приобрели квартиру или собственный дом, осуществили ремонт и благоустройство уже имеющейся недвижимости. Широко разветвленная структура банка включает в себя филиалы в Москве, Санкт-Петербурге, Екатеринбурге, Ростове-на-Дону, Новосибирске и еще восемнадцати регионах Российской Федерации.



показало, что среди трех сотен просканированных компьютеров не оказалось ни одного, который бы на 100% удовлетворял критериям базы уязвимости. Причина заключалась в том, что у ИТ-администраторов не было адекватного инструмента, позволяющего получить информацию об установленных пакетах обновлений, о членстве пользователей в группе локальных администраторов и так далее. Владимир Максимов так прокомментировал ситуацию: «Когда речь идет об удаленных офисах, распространенной ошибкой становится наличие большого количества пользователей в группе локальных администраторов отдельных компьютеров. В нашей практике мы часто сталкиваемся с подобными нарушениями системы безопасности». По мнению представителей банка, важной оказалась возможность создания собственных критериев уязвимости в рамках системы LANDesk, например, наличие определенного файла или записи в реестре.

БЕЗОПАСНОСТЬ И АУТСОРСИНГ

Как мы уже говорили, особенностью внедрения технологий LANDesk в Городском Ипотечном Банке стала передача процессов технической поддержки и обслуживания компьютерной техники заказчика на аутсорсинг специализированной компании. В этом случае особенно актуальными становятся вопросы безопасности. ИТ-отделу банка данное внедрение позволило убить сразу двух зайцев: во-первых, LANDesk предоставила мощный инструментарий для аутсорсинговой компании, позволяющий производить мониторинг состояния компьютерного парка, устанавливать программы и пакеты обновлений, сканировать и исправлять уязвимости, собирать статистику использования программного обеспечения, а также подключаться к рабочим столам пользователей для технической поддержки. Во-вторых, установка LANDesk избавила от необходимости предоставлять специалистам службы технической поддержки права администраторов — как в домене, так и на компьютерах. Более того, инструментарий системы позволяет специалисту ИТ-поддержки только видеть экран сотрудника и рисовать на нем стрелочки и другие графические символы. Благодаря этому сотрудники банка быстрее обучаются самостоятельно решать проблемы с компьютером, а инженеры технической

IDC STORAGE, VIRTUALIZATION AND DATACENTERS EFFICIENCY ROADSHOW 2009

Компания IDC приглашает вас принять участие в конференции «Системы хранения данных, виртуализация и эффективность ЦОД»

22 апреля, Москва, гостиница «Рэдиссон Славянская»

Дополнительная информация и регистрация:
www.idc-cema.com/events/itsecurity09ru

Информационная поддержка

Реклама

1 апреля 2009 г., Москва, отель «Марriott Тверская»

V ВСЕРОССИЙСКАЯ КОНФЕРЕНЦИЯ «ИТ-АУТСОРСИНГ 2009»

Серебряный спонсор:

High performance. Delivered.

ОСНОВНЫЕ ТЕМЫ КОНФЕРЕНЦИИ:

- **ФОКУС-ТЕМА:** Управление рисками в аутсорсинговых проектах.
- **ФОКУС-ТЕМА:** ИТ-аутсорсинг в Госсекторе.
- Тенденции на рынке ИТ-аутсорсинга: требования рынка, возможности подрядчиков и потребности клиентов.
- Аутстаффинг, аутсорсинг или штатный сотрудник? Что выгоднее в условиях кризиса?
- Как свести к минимуму операционные затраты при использовании ИТ-аутсорсинга?

- Специфика аутсорсинга в сегменте информационной безопасности.
- Потенциал модели SaaS в области аутсорсинга.
- **БИЗНЕС-КЕЙС:** Аутсорсинг Центра обработки данных.
- Практические аспекты построения успешной схемы взаимодействия заказчик – сервис-провайдер при аутсорсинге.
- Рост спроса на виртуализацию как новый тренд 2009 года.
- Отраслевая специфика ИТ-аутсорсинга: опыт компаний.

Официальный информационный партнер:

Аналитический информационный партнер:

Информационные партнеры:

Зарегистрируйтесь на мероприятие:
по телефону +7 (495) 234-0588 • e-mail: IT@ahconferences.com
на сайте www.ahconferences.com

Реклама

НОВОСТИ

DIRECTUM ПРЕДЛАГАЕТ ГРАНТ В 3 МЛН РУБЛЕЙ

Стартовал инновационный конкурс компании DIRECTUM, победитель которого получит грант в размере 3 млн рублей.

Цель конкурса — поиск максимально эффективных проектов использования ЕСМ-систем для повышения результативности бизнеса.

Конкурс пройдет в онлайн-режиме (на сайте grant.directum.ru) в три этапа. В рамках первого — он продлится до 31 мая — участники смогут заявить свои проекты. В течение двух недель после этого экспертный совет решит, проходит ли данный проект во второй этап. Далее, на втором этапе (до 19 июня), необходимо направить в экспертный совет уточняющую документацию по проекту (техзадание, спецификацию и т. д.). Определение победителя состоится на третьем этапе — его имя будет объявлено 1 июля.

Грант — программное обеспечение и право на проведение работ по внедрению системы DIRECTUM (на сумму до 3 млн рублей) — будет вручен за проект, показавший наилучшие результаты по трем основным направлениям:

- > эффективность: проект должен давать максимальную экономическую отдачу за минимальное время;
- > комплексность: проект должен быть направлен на максимальное развитие инфраструктуры документооборота на предприятии;
- > новизна и перспективность в области применения ЕСМ в целом.

Каталог АСТРА 2009

Комитет по исследованиям и аналитике Ассоциации стратегического аутсорсинга (некоммерческое партнерство «АСТРА») и аналитическое агентство in4media приглашают принять участие в подготовке первого выпуска ежегодного справочно-аналитического издания «Каталог АСТРА 2009: Поставщики услуг IT-Аутсорсинга в России».

Каталог создается как профессиональный бизнес-справочник. На его страницах планируется публиковать обзоры мирового и российского рынка IT-аутсорсинга, статьи и интервью с его представителями, описания кейсов аутсорсинговых контрактов, предложения поставщиков услуг IT-аутсорсинга в России.

поддержки даже теоретически не могут получить доступ к финансовым системам. Все действия специалистов аутсорсинговой компании протоколируются, руководство ГИБ в любой момент может получить полную отчетность.

Во всей сети банка были реализованы новые возможности контроля на уровне операционной системы, что позволило ограничить сотрудников в копировании информации — на всех компьютерах заблокирована возможность подключения съемных носителей и запись на оптические диски.

Гибкая система установки обновлений операционных систем и приложений позволила избежать ситуаций, когда установка очередного обновления операционной системы увеличивает время загрузки компьютера до десятков минут, принудительно перезагружает компьютер не давая пользователю выполнить срочную работу.

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

Уже сегодня специалисты банка обеспечивают полный мониторинг как состояния сети, так и деятельности аутсорсинговой компании, выполняющей обслуживание и поддержку. Автоматические инструменты LANDesk контролируют состояние различных пакетов ПО по ежедневно обновляемой базе уязвимостей продуктов популярных вендоров, а также по критериям, формируемым администраторами системы.

Функционирование системы LANDesk в случае с удаленными филиалами может происходить по различным каналам связи. Благодаря грамотным настройкам, как бы далеко ни находились компьютеры, ПО эффективно работает даже по медленным каналам связи (от 9600 бит/с), а также по каналам с большими задержками (до 5000 мс), поддерживая настройку прав доступа на основе ролей. Что касается установки обновления ПО, то этот процесс происходит централизованно, причем с контролем загрузки полосы пропускания каналов связи, отдавая приоритет бизнес-системам и другому трафику, при этом выделенные ПК в удаленной сети используются как временное хранилище пакетов не требуя выделенных серверов. Благодаря этому в удаленную подсеть передается только одна копия пакета установки или обновления ПО, распределяемая в дальнейшем по всем целевым ПК.

Еще одна интересная возможность, используемая сотрудниками банка, — восстановление после сбоя с помощью функционала развертывания операционных систем. Готовый образ уже хранится на центральном сервере, и в случае сбоя или ввода в строй нового компьютера администратору нужно лишь запустить удаленную заливку, нажав всего одну клавишу. В процессе установки LANDesk автоматически установит необходимые драйверы, обеспечив работу универсального образа на любых аппаратных конфигурациях.

Еще одна интересная возможность, используемая сотрудниками банка, — восстановление после сбоя с помощью функционала развертывания операционных систем

ПЕРСПЕКТИВЫ

В полной мере оценив возможности установленной системы, специалисты ГИБ заинтересовались перспективами функционала подсистемы LANDesk HIPS (LANDesk Host Intrusion Prevention System). LANDesk HIPS контролирует работу программ и блокирует любую неавторизованную активность, что особенно важно для предприятий финансового сектора. В отличие от технологии сканирования с использованием цифровых подписей, которая применяется во многих антивирусных и антишпионских решениях, LANDesk Host Intrusion Prevention использует не только уже существующие подписи и файлы с шаблонами для идентификации вредоносного ПО. В HIPS заложена технология, которая анализирует поведение сервисов и прикладных программ для определения аномалий или случаев нарушений политики безопасности на основе правил, определяемых администраторами безопасности, таких как попытка записи в реестр, доступ к накопителям, попытка передачи данных по сети и другие. В настоящий момент специалисты ГИБ проводят ее тщательное тестирование.