

# КОРПОРАТИВНАЯ МОБИЛЬНОСТЬ: ХОРОШО ИЛИ ПЛОХО?

АЛЕКСЕИ ДОЛЯ

ТЕКСТ



СОГЛАСНО НЕДАВНЕМУ ОПРОСУ, ПРОВЕДЕННОМУ В США И ЕВРОПЕ КОМПАНИЕЙ DYNAMIC MARKETS, БОЛЬШАЯ ЧАСТЬ КОМПАНИЙ НЕ СПОСОБНА ПРОТИВОСТОЯТЬ ВОЗРАСТАЮЩИМ УГРОЗАМ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ ВНЕ КОРПОРАТИВНОЙ СЕТИ. ВЗЛОМЫ ЧАСТО ЯВЛЯЮТСЯ РЕЗУЛЬТАТОМ НЕДОСТАТКОВ КОРПОРАТИВНОЙ ПОЛИТИКИ ПРЕДОТВРАЩЕНИЯ ПОДКЛЮЧЕНИЙ НОУТБУКОВ И ДРУГИХ МОБИЛЬНЫХ СИСТЕМ В СЕТЬ БЕЗ СООТВЕТСТВУЮЩИХ ПРОВЕРЕК БЕЗОПАСНОСТИ ДОСТУПА.

Более 65% опрошенных IT-менеджеров отметили, что их компании подвергаются взломам, и помимо антивирусного программного обеспечения им приходится искать дополнительные меры защиты. 60% респондентов сказали, что их организация не имеет возможности сканировать компьютеры, пытающиеся подключиться к их сети и отсекают любую систему, которая не удовлетворяет требованиям безопасности их компании. Почти половина опрошенных (46%) отметила, что настроить параметры безопасности на ноутбуках и других мобильных системах возможно только когда эти системы физически возвращаются в корпоративную среду. Это означает, что когда они работают и подключаются удаленно, они представляют существенный риск для бизнеса.

[001] Не только европейские, но и российские компании недооценивают серьезность угроз, связанных с применением их сотрудниками мобильных приложений. По некоторым оценкам, примерно 70% сотрудников крупных компаний в качестве основных рабочих инструментов используют ноутбуки. Работники, находящиеся вне офиса или перемещающиеся по служебным помещениям, зачастую прибегают к помощи карманных компьютеров, смартфонов и сотовых телефонов. Корпоративные IT-службы обычно не контролируют устанавливаемое на таких устройствах программное обеспечение и их уровень безопасности. Аналитики Gartner считают, что 90% мобильных устройств не имеют серьезных механизмов защиты. Понятно, что в условиях роста числа угроз все это ведет к нарушениям целостности информационных систем.

**[000]** Идея комплексного подхода к защите сети появилась не на пустом месте, так как сегодня необходимо защищать и конфиденциальную информацию, и саму сеть практически от всего, что можно придумать: от вирусов, троянцев, червей, злоумышленников и, наконец, самих пользователей. Кроме того, данные надо защищать не только в силу вредоносности того или иного ПО, но также несовершенства привычных для сотрудника продуктов. И если такая задача ставится перед IT-отделом, обслуживающим парк из более 100 компьютеров, IT-директору остается либо хвататься за голову, либо задуматься о внедрении единой системы управления безопасностью сети. Управление безопасностью тесно связано с задачами управления всей информационной системой: инвентаризацией ПО, конфигурированием систем, установкой и обновлением программного обеспечения и др. LANDesk Software одной из первых начала внедрять в программные продукты управления инфраструктурой предприятия (LANDesk Management Suite, LDMS) элементы управления безопасностью корпоративной сети.

Разработанный компанией продукт LANDesk Security Suite (LDSS) включает систему управления обновлениями Patch Manager, модуль защиты от шпионских и рекламных программ

ржки инфраструктуры, например, HelpDesk, что делает его удобным как с точки зрения использования, так и с позиции администрирования. Во-вторых, LDSS контролирует доступ к сети, независимо от того, имеется на конкретном компьютере программный агент LANDesk или нет, что позволяет перейти на принципиально другой уровень управления безопасностью в сети.

Использование LANDesk Security Suite 8.6 ведет к нескольким преимуществам, которые будут очевидны даже без тонкой настройки системы. Во-первых, использование серверной инфраструктуры и интеграция с системами управления сетью позволяет LDSS применять заданные политики безопасности одновременно на всех компьютерах, уже включенных в сеть и сразу отслеживать соответствие политикам только что подключившихся компьютеров. Компонент LANDesk Security Suite, занимающийся поиском угроз, — Threat Analyzer — проверяет, кто входит в группу администраторов и насколько это соответствует принятой на предприятии политике безопасности. Компонент определяет, какие каталоги доступны для монтирования извне и насколько это санкционировано. Он же следит за тем, какие сетевые сервисы доступны внешнему пользователю

## ЕВРОПЕЙСКИЕ И РОССИЙСКИЕ КОМПАНИИ НЕДООЦЕНЯЮТ СЕРЬЕЗНОСТЬ УГРОЗ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ИХ СОТРУДНИКАМ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ...

Spyware Detection and Removal, анализатор угроз безопасности Threat Analyzer, систему обнаружения и блокирования несанкционированных приложений Application Blocker, модуль поиска новых дефектов User-defined Vulnerabilities, систему управления доступом Connection Control Manager, модуль собственного обновления LANDesk Update, а также технологию Trusted Access, которая не допускает подключения к информационной системе непроверенных компьютеров. Данный пакет программ может быть установлен как самостоятельно, так и совместно с системой управления LANDesk Management Suite.

LANDesk Security Suite 8.6 (LDSS) используется в сетях различных компаний благодаря тем же преимуществам, что и LANDesk Management Suite. Продукт можно развернуть в кратчайшие сроки на сети от нескольких десятков до нескольких тысяч ПК, его просто поддерживать и интегрировать с другими системами подде-

и насколько это оправданно. Threat Analyzer проверяет работу контролера домена, доступность гостевого входа, работу межсетевых экранов, качество паролей, версии операционных систем, уровень безопасности браузеров и многое другое, что может являться признаком успешно завершенной атаки. Во-вторых, LANDesk Security Suite 8.6 обладает не только возможностями обнаружения уязвимостей, но и модулем, отвечающим за их автоматическое устранение. Система Patch Manager включает в себя эффективный механизм проверки установленных программных пакетов на наличие уязвимостей, сверяясь с постоянно обновляемой базой данных LANDesk, а также механизм автоматизированного развертывания обновлений во всей сети для всех заданных программных пакетов. Также LANDesk Security Suite может отслеживать наличие потенциально опасных настроек в популярных программных продуктах, например, в том же Microsoft Office



### FrontRange Solutions: новое позиционирование на рынке

Компания FrontRange Solutions провела в Москве пресс-конференцию, посвященную представлению стратегии своей работы после приобретения компании группой Francisco Partners.

Пресс-конференцию открыл вице-президент по разработке Call-центров FrontRange Solutions Константин Кишинский. По его словам, в ближайшее время ожидается агрессивный рост компании и усиление ее финансовых показателей.

К началу 2006 года количество пользователей продуктов компании превысило 140 тысяч. Офисы и центры разработки расположены в Европе, Северной и Южной Америке, Африке и Австралии, а общее число сотрудников превышает 400 человек (50 из них работают в России).

По словам Константина, FrontRange Solutions создает новое поколение бизнес-приложений для построения системы обслуживания, системы взаимоотношений с клиентами. Г-н Кишинский заострил внимание на том, что решения имеют кратчайшие сроки внедрения и возврата инвестиций, низкую стоимость владения, а также гибки и просты в использовании.

На пресс-конференции был представлен ряд продуктов, которые компания предлагает российским заказчикам, — это ПО для организации службы сервисной поддержки, создания распределенного контакт-центра и автоматизации его работы, а также CRM-приложение Goldmine. Отметим, что все программы базируются на единой платформе и хорошо интегрируются друг с другом.

FrontRange Solutions держит курс не только на расширение линейки продуктов, а также модернизацию старых решений, создание новых модулей для уже работающих систем на HEAT и GoldMine. В ближайшее время ожидается выпуск дополнительных инструментов, которые помогут наиболее безболезненно и наименее хлопотно перейти на новые версии продуктов. В нынешнем году компания также надеется поправить свои финансовые показатели, оптимизировать поставленную стратегию удержания существующих клиентов и увеличения своего присутствия на растущих и крупных рынках. Планируется усиление команды — в нее будут приглашены топ-менеджеры отрасли.

## защита как стиль бизнеса



### Terrasoft: индивидуальная CRM-система

25 апреля 2006 года состоялся релиз нового продукта Terrasoft CRM 3.0 — комплексной CRM-системы, покрывающей весь спектр коммерческих задач предприятия.

В основе Terrasoft CRM 3.0 лежит платформа, позволяющая создавать конфигурации, строго соответствующие бизнес-задачам клиента. Платформа поставляется с любой конфигурацией продукта, что дает клиенту возможность разработать собственное CRM-решение.

Возможна поставка продукта в двух стандартных конфигурациях. Terrasoft CRM X15 содержит базовый набор функциональности. В поставку входит 15 модулей. Terrasoft CRM X25 — комплексная CRM-система, покрывающая весь спектр коммерческих задач предприятия (продажи, маркетинг, сервис, управление ресурсами). В поставку входит 25 модулей. Пользователи могут приобрести X15 и в любой момент перейти на X25, оплатив разницу в цене лицензий. Кроме того, все желающие могут перейти с версии 2.x на 3.0. Версия 2.x будет по-прежнему поддерживаться.

### Сервис-пакет для IT Service Management 5.0.4

Компания FrontRange Solutions выпустила новую версию своего модульного продукта IT Service Management (ITSM).

Service Pack 1 устанавливается на версию ITSM 5.0.4. Новая версия ITSM имеет клавиши быстрого вызова команды и различные варианты настройки. Среди других нововведений: появление опции Presence Management (контроль присутствия), позволяющей определять присутствие оператора на рабочем месте; усовершенствование Wizard-мастера для поддержки совмещения версии 5.0.4 с предыдущими версиями; улучшение Inventory Management, включая утилиту сравнения учетных элементов (CI Comparison Utility), опции Inventory Identity, Discovery Enhancements и Scheduled Jobs.

Комментирует Лори Самолик (Lori Samolyk), старший менеджер по маркетингу компании FrontRange: «Все усовершенствования повышают функциональность комплекса ITSM как продукта класса предприятия. ITSM дает возможность представителям крупного и мелкого бизнеса управлять своими ИТ-системами и процессами в соответствии с принципами ИТIL».



LANDesk Software внедряет в программные продукты управления инфраструктурой предприятия элементы управления безопасностью корпоративной сети



Тема

## ИДЕЯ КОМПЛЕКСНОГО ПОДХОДА ПОЯВИЛАСЬ НЕ НА ПУСТОМ МЕСТЕ, ТАК КАК СЕГОДНЯ НЕОБХОДИМО ЗАЩИЩАТЬ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ И САМУ СЕТЬ...

и препятствовать их активизации. То есть, при возникновении опасных ситуаций, LDSS исправит неверные настройки, если такое исправление возможно, удалит обнаруженное шпионское или любое другое вредоносное ПО, а также не даст запустить запрещенные приложения, даже если компьютер в данный момент не подключен к сети. В результате, при использовании LDSS администратору не придется тратить время на восстановление пострадавших систем при появлении новой угрозы или же заниматься обновлением того же Microsoft Office на всех компьютерах – LDSS сделает это самостоятельно и предоставит администратору подробный отчет. Когда речь идет о компьюте-

рах, поддерживающих технологию Intel AMT, восстановление компонентов может происходить за счет автономного управления, реализованного в платформе Intel. В этом случае возможно также восстановление операционной системы Windows или любой другой, даже если компьютер вообще не хочет загружаться. Конечно, при неисправности или отсутствии, например, процессора или оперативной памяти восстановление системы провести не удастся, но обнаружение отсутствия этих компонентов вполне возможно средствами LANDesk. Технология Intel AMT реализована как подсистема, полностью независимая от операционной системы компьютера. Эта независимость решает

## защита как стиль бизнеса

одну из главнейших проблем современного IT-персонала: преднамеренное или случайное отключение функций безопасности и управления на ПК и мобильных устройствах.

Отдельно стоит рассмотреть технологию Trusted Aces, реализованную в системе LANDesk. Она позволяет ограничивать компьютеры, не соответствующие корпоративным политикам безопасности в возможностях доступа к сети. И, что приятно, речь идет не только о том, удовлетворяет ли пользователь требованиям или нет – система определяет, насколько актуальны базы антивирусного ПО на данном компьютере, какие программы установлены, но и требуются ли компьютеру обновления компонентов для каких-либо программных пакетов. По результатам проверки возможно включение его в карантинную сеть, где и будет происходить обновление компонентов и, например, проверка на вирусы. И только после этого компьютер будет подключен к основной корпоративной сети. Этот механизм может работать как самостоятельно, так и пользоваться аппаратной поддержкой Cisco NAC (Network Admission

Control). Все это происходит как с установленным программным агентом на конкретном компьютере, так и без него. В результате, если речь идет о подключении к сети портативного компьютера, например удаленного пользователя через VPN или же приходящего консультанта в локальной сети, пользователю будет предложено выполнить все необходимые обновления и после этого попробовать получить доступ еще раз. Не сделав этого, пользователю придется довольствоваться лишь подключением к Интернету или же к определенному разделу сети.

Средствами LANDesk Security Suite можно ограничивать для каждого пользователя или компьютера доступ к портам или дисководам, либо запретить, например, использование модемов или других средства связи, таких как беспроводные сетевые карты или устройства Bluetooth, что снижает возможность утечки информации. Ведь даже если речь не идет о внутреннем шпионаже, это могут быть просто ошибки пользователей. В рамках консоли LDSS можно также ограничить доступ к IP-адресам

в локальной сети или Интернете, определив свои политики для каждой группы компьютеров. В дополнение администратор может прямо из консоли LANDesk управлять настройками корпоративного антивируса, а также стандартного firewall, входящего в состав любой версии Windows XP SP2 на каждом компьютере в отдельности применительно к группе компьютеров.

Подводя итог сказанному, отметим, что LANDesk Security Suite 8.6 позволяет менять политику использования данных во всей сети «одним щелчком мыши». Например, одним таким действием можно отключить возможность использования USB-брелков во всей сети или для одного подразделения либо же запретить использование того или иного ПО для любого компьютера. Целесообразность внедрения LANDesk Security Suite 8.6 не останется непонятой для руководства – в любой момент система может выдать отчет о своей деятельности и о достигнутых успехах, что значительно облегчает отчетность IT-отдела при внедрении этого продукта. ☒