

## Интегрированное решение LANDesk Security Suite, Cisco NAC и Intel AMT как средство защиты корпоративной сети

**С**огласно недавнему опросу, проведенному в США и Европе компанией Dynamic Markets, большая часть компаний неспособны противостоять возрастающим угрозам при использовании мобильных устройств вне корпоративной сети. Взломы часто являются следствием недостатков корпоративной политики безопасности, не предусматривающей соответствующих проверок при подключении ноутбуков и других мобильных систем в сеть.

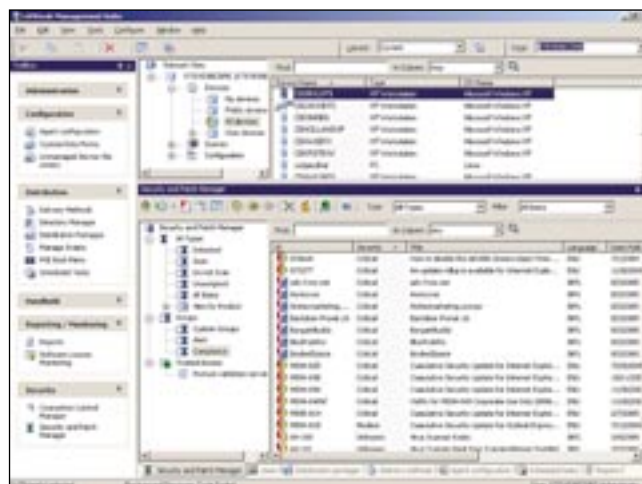
Более 65 % опрошенных IT-менеджеров указали, что их компания подвергается взломам, и помимо антивирусного программного обеспечения им приходится искать дополнительные меры защиты. 60 % респондентов сказали, что их организация не имеет возможности сканировать компьютеры, пытающиеся подключиться к их сети, и соответственно отсекают системы, не удовлетворяющие 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 при удаленном подключении они представляют существенный риск для бизнеса.

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 основного рабочего инструмента используют ноутбук. Работники, находящиеся вне офиса или перемещающиеся по служебным помещениям, активно используют карманные компьютеры, смартфоны и сотовые телефоны. 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.

Идея комплексного подхода к защите корпоративных сетей 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 по при-

ичне вредоносности того или иного ПО, но также и вследствие 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 серьезно 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 т.д.. Компания LANDesk Software одной из первых уловила назревшие потребности и включила в свой основной продукт по управлению IT-инфраструктурой – 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 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 сам по себе, так и совместно с системой управления LANDesk Management Suite.



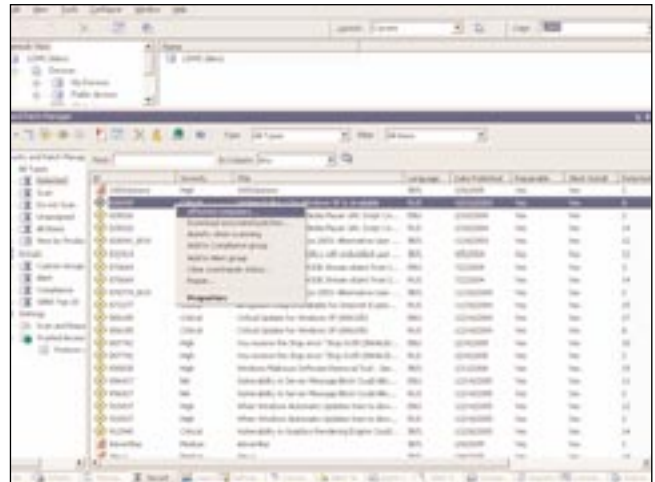
LANDesk Security Suite 8.6 используется в сетях различных компаний благодаря тем же преимуществам, что и LANDesk Management Suite. Продукт можно развернуть в кратчайшие сроки на сети от нескольких десятков до нескольких тысяч ПК, его просто поддерживать и интегрировать с другими системами поддержки инфраструктуры, например, HelpDesk, что делает его удобным как с точки зрения использования, так и 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 иной уровень управления безопасностью в сети.

Использование LANDesk Security Suite 8.6 дает очевидные преимущества даже и 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 разрешены для доступа внешнему пользователю и насколько это оправданно. Threat Analyzer проверяет работу контроллера домена, доступность гостевого входа, работу межсетевых экранов, качество паролей, версии операционных систем, уровень безопасности браузеров и многое другое, что может являться признаком успешно завершённой 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 отслежи-

вать наличие потенциально опасных настроек в популярных программных продуктах, например, в том же Microsoft Office, 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 Microsoft Office на всех компьютерах – LDSS сделает это самостоятельно и предоставит администратору подробный отчет. Когда речь идет о компьютерах, 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 одну из главных проблем современного IT-персонала: устраняет возможность преднамеренного или случайного отключения функций обеспечения безопасности и управления на ПК и мобильных устройствах.

Однако, истинным шедевром управления безопасностью, который реализован в системе LANDesk, может считаться технология Trusted Access. Данная разработка позволяет ограничивать компьютеры, не соответствующие корпоративным политикам безопасности в возможностях доступа к сети. И что существенно, система не только определяет, удовлетворяет ли конкретный пользователь требованиям или нет, насколько актуальны базы антивирусного ПО на данном компьютере, какие программы уста-



новлены, но и также, 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. Особенность Cisco Network Admission Control в том, что система проверяет не только стандартные «логин-пароль», но и осуществляет процедуру идентификации самого ПК, сравнимую с проверкой паспорта на пограничном контроле. Она направлена, прежде всего, не на защиту «объекта атаки», а на изоляцию «атакующего» субъекта. При этом Cisco NAC эффективна при любом способе загрузки «злоумышленника», включая системную загрузку с компакт-диска или флеш-карты.

Эта технология также обеспечивает двустороннее согласование политик сервера контроля доступа Cisco Secure ACS и ядра системы LANDesk. Таким образом, при правильной настройке окружения опасный компьютер, например, не имеющий актуального антивирусного ПО, не просто изолируется на уровне IP-трафика, но попадает вообще в другую сеть, в которой он может либо пользоваться только Интернетом, либо скачать необходимые программы и обновления, для того чтобы соответствовать уровню корпоративных политик безопасности. 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. Если пользователь не делает этого, ему придется довольствоваться лишь подключением к Интернету или же к определенному разделу сети.

Обе технологии решают вопросы более полного контроля за соблюдением корпоративных политик на всех узлах сети, а также простого распространения как ПО, так и политик безопасности для сети любого масштаба. В том или другом случае администратор, использующий возможности Cisco NAC, Intel AMT и LDMS, способен узнать о компьютере сотрудника гораздо больше а также эффективно управлять им, даже если это ноутбук топ-менеджера, находящегося в командировке.

Средствами LANDesk Security Suite можно ограничивать для каждого пользователя или компьютера доступ к портам и дисководам, или запретить, например, использование модемов и других средств связи, таких как беспроводные сетевые карты или устройства Bluetooth, что снижает возможность утечки информации. Ведь даже если речь не идет о внутреннем шпионаже, это может произойти и из-за ошибок 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 сети «одним щелчком мыши». Например, одним таким действием можно отключить возможность использования USB-брелков во всей сети или для одного подразделения или же запретить использование того или иного ПО для любого компьютера. Целесообразность внедрения LANDesk Security Suite 8.6 достаточно очевидна и 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.

*По материалам компании Arbyte*