

## Под щитом управления

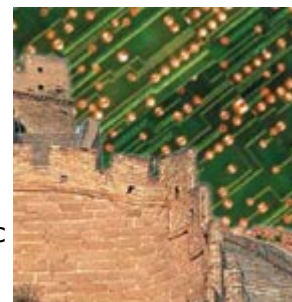
Валерий Коржов

13.06.2005

Открытые системы, #05-06/2005

**Ни один, даже самый совершенный программный продукт не может обеспечить необходимую предприятию защиту от различных угроз — слишком они разнообразны и изощрены. Для полноценной защиты требуется комплексное решение, которое позволило бы обеспечить защиту вычислительной системы со всех направлений.**

Интегральное решение по обеспечению безопасности должно заниматься поиском вирусов и шпионских программ, мониторингом происходящих в системе процессов, инвентаризацией устройств и их первоначальной настройкой, определением их уязвимости, организацией доступа к ним и управлением обновлениями. Однако перечисленные задачи должны решаться уже не средствами защиты, которые реализуют определенные защитные политики, а с помощью системы управления жизненным циклом корпоративных приложений Security Management.



## Управление — основа безопасности

Традиционные системы защиты работают по определенным правилам, установленным администратором и позволяющим автоматизированным системам выделить и предотвратить опасные ситуации. Весь свод корпоративных правил защиты формирует политику безопасности предприятия, определить которую достаточно сложно, однако без ее строгой детализации современные защитные механизмы будут нежизнеспособны. По этим принципам работают сетевые экраны, детекторы дефектов и нападений, антивирусы, информационные фильтры и многие другие продукты, обеспечивающие информационную безопасность. Однако можно пойти по другому пути — обеспечивать нормальное функционирование установленных на предприятии приложений.

Управление приложением тесно связано с его жизненным циклом: установка, настройка, штатная работа, обновление и вывод из эксплуатации, возможно, с заменой на новое. Понятно, что каждый из этих этапов может быть использован злоумышленником для вмешательства в корректную работу системы, поэтому компаниям нужно предусмотреть адекватные механизмы защиты и контроля. Это означает, что система управления безопасностью должна иметь следующие компоненты:

- средство инвентаризации установленного программного обеспечения и утилиты установки и настройки приложений;
- механизмы контроля доступа к приложениям;
- утилиты для выявления возможных уязвимостей и нападений;
- система мониторинга работы приложений;
- приложения для поиска программ, неэффективно расходующих системные ресурсы, таких как вирусы и шпионские программы;
- система обновления.

Поскольку фаза штатной работы наиболее продолжительная, то и приложений для ее защиты может быть несколько. Они контролируют самые разнообразные аспекты вычислительного процесса: доступ пользователей, поиск признаков нападения, контроль работы приложений и выявление лишних приложений. Эти утилиты контроля должны работать постоянно, и часто являются неотъемлемой частью защищаемого

приложения. В то же время начальная установка и настройка, а также развитие и вывод приложений из строя вполне могут обойтись одной утилитой, которая к тому же запускается не часто. Тем не менее это не значит, что последним этапам не стоит уделять внимания, наоборот, правильная первоначальная настройка и вовремя сделанное обновление могут существенно улучшить положение программы во время ее эксплуатации.

Следует отметить, что современные корпоративные приложения уже не работают на одном компьютере, а представляют собой цепочку из нескольких внешне независимых и физически распределенных программных элементов. Однако изменение в одном из них может разрушить всю систему, поэтому компании должны уделять внимание различным компонентам вычислительной системы, включая все устройства, составляющие корпоративную систему: серверы, рабочие станции, персональные устройства и сетевое оборудование. Однако поддержание работоспособности данных устройств входит в задачу управления системами, с которой должна тесно интегрироваться задача управления безопасностью. Современные приложения управления безопасностью как раз и пришли из мира управления системами. Среди тех, кто предлагает сегодня решения этого класса, можно назвать Microsoft, LANDesk, BMC Software и ряд других компаний. Показательно, что Microsoft в настоящее время чрезвычайно активно наступает на рынок средств обеспечения безопасности, причем по целому ряду направлений; среди ключевых направлений — решение проблем эффективного расходования вычислительных ресурсов. Другие производители этой группы также начинают выпускать свои продукты, предназначенные для обеспечения комплексной информационной безопасности корпоративных систем. В частности, компания LANDesk выпустила программный инструментальный LANDesk Security Suite, включающий все перечисленные классы утилит управления безопасностью.

## **Управление безопасностью от LANDesk**

Пакет LANDesk Security Suite включает систему управления обновлениями Patch Manager, модуль защиты от шпионских и рекламных программ Spyware Detection and Removal, анализатор угроз безопасности bThreat Analyzer, систему обнаружения и блокирования несанкционированных приложений Application Blocker, модуль поиска новых дефектов User-defined Vulnerabilities, систему управления доступом Connection Control Manager и модуль собственного обновления LANDesk Update. Данный пакет программ может быть установлен как самостоятельно, так и интегрирован в систему управления LANDesk Management Suite.

Компонент управления обновлениями позволяет администраторам определить набор исправлений, уже установленных на подотчетных ему компьютерах, причем Patch Manager определяет не только установленные с его помощью обновления, но и все остальные, например инсталлированные пользователем самостоятельно. Это позволяет удалить обновления, которые признаны ненужными или опасными. Поддерживается работа в средах Windows, Linux (Red Hat, Novell/SuSe) и Mac OS. Сам же Patch Manager предоставляет средства управления автоматической установкой обновлений, например определяя конфигурацию по умолчанию, необходимость перезагрузки после установки обновлений и другое поведение системы в процессе установки.

Модуль защиты от вредоносных программ Spyware Detection and Removal выполняет задачи, связанные с распознаванием, блокировкой, лечением и удалением таких хакерских программ, как «троянские кони», контролеры поведения пользователя и нажатий клавиш на клавиатуре, и других, мешающих работе пользователей и непроизводительно расходующих ресурсы компьютера. Кроме этого, модуль восстанавливает файлы, поврежденные в процессе борьбы с вредоносными программами, и предотвращает повторное заражение вирусами.

Еще один компонент LANDesk Security Suite, занимающийся поиском угроз, — Threat Analyzer. Он 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 санкционированно. Он же следит за тем, какие сетевые сервисы доступны внешнему пользователю и насколько это оправданно. Threat Analyzer проверяет работу контролера домена, доступность гостевого входа, работу межсетевого экрана, качество паролей, версии операционных систем, уровень безопасности браузеров и многое другое, что может являться признаком успешно завершённой атаки.

Если же вирус все-таки проник в систему и начал активно размножаться, то его поведение должен заметить анализатор поведения программ Application Blocker, знающий, какие приложения могут вести себя подозрительно и в чем это выражается. Эти знания могут поступать как от специалистов компании-производителя, так и от самих клиентов, которые лучше понимают особенности поведения установленных у них приложений. Кроме того, компонент определяет и блокирует запуск программ, которые не разрешены политикой безопасности, не являются корпоративным стандартом, уменьшают защищенность или производительность вычислительной системы.

Компонент Connection Control Manager обеспечивает контроль доступа сетевых приложений к ресурсам компьютера. В частности, он ограничивает доступ по сети к таким устройствам, как шина USB, модемы, различные съемные накопители, параллельные и последовательные порты и беспроводные устройства. Этот же компонент контролирует, насколько разрешено то или иное сетевое подключение и в случае нарушения политики безопасности поднимает тревогу.

Модуль LANDesk Updates занимается обновлениями различной информации, связанной с работой Security Suite, в частности устанавливает обновления всех компонентов, входящих в пакет, изменяет правила их работы, а также определяет правила обновления приложений. Различают четыре типа обновлений — ядро, консоль, Web-консоль и клиент; каждый из них относится к соответствующим элементам самого пакета Security Suite. С помощью этого компонента система может постепенно развиваться и настраиваться на отражение новых угроз.

Комплексная работа всех перечисленных утилит создает синергетический эффект. Так традиционные сканеры дефектов пытаются при помощи сетевого сканирования определить уязвимость систем, посылая большое количество тестовых запросов, что в некоторых случаях может перегрузить систему. В средствах управления безопасностью уже есть все необходимые данные для определения уязвимости системы, поскольку в них имеются данные об установленных версиях программного обеспечения и соответствующих исправлениях, поэтому таким системам не требуется проводить сканирование ресурсов. Как только в ней появляются сведения о найденных дефектах с подробной информацией об уязвимых версиях, система может без сканирования определить, какой именно компьютер наиболее уязвим к данной атаке. А если для дефекта выпущено исправление, то комплексное приложение тут же его установит.

## **Системное управление**

Система управления безопасностью часть утилит унаследовала из продукта LANDesk Management Suite, который предназначен для централизованного управления различными компонентами информационной системы. В частности, система управления обновлениями, утилиты инвентаризации и базовой настройки приложений включены в оба продукта LANDesk. Тесная интеграция Security Suite с этим пакетом позволит расширить возможности обоих.

Management Suite — решение по комплексному управлению информационной системой предприятия, нацеленное на выполнение следующих задач:

- средства управления серверами (Server Management);

- инструментарий установки и настройки операционных систем (OS Imaging & Migration);
- установка программного обеспечения (Software Distribution);
- управление лицензиями (Software License Monitoring);
- удаленный контроль и техническая поддержка (Remote Control/Problem Resolution);
- подготовка отчетов (IT Asset Management);
- управление обновлениями (Patch Management).

Каждая утилита в отдельности выполняет возложенную на нее задачу, а все вместе они управляются с единой консоли и используют централизованное хранилище с данными по конфигурации системы. По сути, этот пакет является модульным, и к нему можно добавлять новую функциональность.

Для расширения базовой функциональности предлагаются дополнительные модули для управления обновлениями Patch Manager (входит в состав Security Suite), серверами Server Manager и персональными устройствами Handheld Manager. Среди дополнительных модулей имеется средство мониторинга System Manager, позволяющее контролировать поведение присутствующих в системе программ. В качестве модулей к Management Suite могут подключаться и другие компоненты Security Suite, что позволяет интегрировать систему управления безопасностью в общую стратегию управления ИТ в компании.

Пакет LANDesk Management Suite рассчитан на использование в информационных системах различных размеров; в частности, пакет может быть интегрирован в сложную корпоративную инфраструктуру с несколькими филиалами, соединенными с центральным офисом медленными каналами. Для оптимизации трафика, который в этом случае может передаваться по платным каналам, можно использовать технологию Targeted Multicast, позволяющую компании оптимизировать рассылку обновлений и больших пакетов программ при использовании медленных каналов связи. Имеется и другая технология оптимизации, Peer Download, суть которой заключается в том, что обновления и программное обеспечение можно получить не только с центрального сервера системы, но с любого устройства, на которое эти обновления уже были установлены. Таким образом, в этом фрагменте корпоративной сети распространение программного обеспечения можно организовать, не задействуя внешние каналы.

**\*\*\***

Безопасной считается не та информационная система, которую невозможно взломать, — таких систем не бывает, — но та, которая позволяет сотрудникам эффективно и оперативно выполнять свои функции, не отвлекая их от основной работы. Именно для этого и предназначены системы управления безопасностью.