



ЗАЩИТА УПРАВЛЕНЦЕМ

У СИСТЕМ БЕЗОПАСНОСТИ ЕСТЬ ОДИН ГЛАВНЫЙ ПРИНЦИП: ИНФОРМАЦИОННАЯ СИСТЕМА (ИС) ПРЕДПРИЯТИЯ ЗАЩИЩЕНА НАСТОЛЬКО, НАСКОЛЬКО ЗАЩИЩЕНО ЕЕ САМОЕ СЛАБОЕ ЗВЕНО. КАК СЛЕДСТВИЕ, У ИС ПРЕДПРИЯТИЯ НЕ ДОЛЖНО БЫТЬ СЛАБЫХ МЕСТ. БОЛЕЕ ТОГО, ЧТОБЫ ПОСТОЯННО ПОДДЕРЖИВАТЬ УРОВЕНЬ БЕЗОПАСНОСТИ КОМПАНИИ, ЕДВА ЛИ ДОСТАТОЧНО УПРАВЛЯТЬ ТОЛЬКО ИНСТРУМЕНТАМИ ИНФОРМАЦИОННОЙ ЗАЩИТЫ. ВАЖНО ЕЩЕ И КОНТРОЛИРОВАТЬ ВСЮ КОНФИГУРАЦИЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ. ИМЕННО ПОЭТОМУ ПОЯВИЛАСЬ ТЕНДЕНЦИЯ СРАВНИВАТЬ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТОЙ С ВЫЧИСЛИТЕЛЬНЫМИ РЕСУРСАМИ — РАБОЧИМИ СТАНЦИЯМИ, СЕРВЕРАМИ И МОБИЛЬНЫМИ КОМПЬЮТЕРАМИ.

ВАЛЕНТИН СЕДЫН

ТЕКСТ

Ошибки в конфигурировании приложений и компонентов информационной системы часто приводят к тому, что у злоумышленников появляется шанс проникнуть в систему. Ключи и пароли малой разрядности, использование паролей и конфигураций по умолчанию, отсутствие шифрования, наличие на серверах неиспользуемых сервисов и приложений — все это относится к компетенции системы управления, но одновременно упрощает задачу взломщика. К тому же и защитные механизмы должны «знать», что они, собственно, защищают, и не реагировать на атаки, которые не могут сработать просто потому, что в системе нет атакуемого сервиса. В результате информация из системы управления увеличивает эффективность работы средств информационной безопасности.



Информационная безопасность выступает как необходимый компонент системы управления компьютерным парком: рабочими станциями, серверами и мобильными компьютерами

Однако и саму информационную безопасность нужно рассматривать в контексте жизненного цикла информационной системы, поскольку атаки приводят к непроизводительному расходованию ресурсов системы и, как следствие, к необходимости наращивать вычислительные мощности компьютеров, емкости каналов и количество серверов. Соответственно, безопасность выступает как необходимый компонент системы управления компьютерным парком: рабочими станциями, серверами и мобильными компьютерами. Таким образом, объединение систем управления вычислительными ресурсами и информационной безопасностью в единый комплекс продуктов улучшит работу каждого из них.

Приведем несколько примеров. До недавнего времени предполагалось, что система установки обновлений относится только к ведению систем управления клиентскими компьютерами (Client System Management — CSM). Но, как показывает практика, новые версии вирусов появляются через несколько недель, или даже дней, после выпуска обновлений, предназначенных для исправления выявленных дефектов системы безопасности. В результате пользователи, не успевшие обновить свое программное обеспечение к моменту появления вируса или червя, который использует для своего размножения найденный дефект, подвергают немалой угрозе свою информационную систему. Получается, что и автоматизированная система установки исправлений неожиданно превращается в значимый элемент обеспечения информационной безопасности и в средство защиты от вирусов.

Кстати, сейчас, чтобы обмануть средства защиты, злоумышленники все чаще прибегают к интересному приему — установке легальных сервисов на атакуемый компьютер. Например, если с помощью какого-нибудь ухищрения установить на компьютер стандартный FTP-сервер, ни один антивирус не расценит его как вредоносное ПО. А между тем появление на компьютере открытого FTP-шлюза создает серьезную брешь в защите информационной системы. Причем использование такого приема практикуется сегодня сплошь и рядом — от sruware и adware ПО до условно бесплатных программ. Все они так или иначе паразитируют на вполне легальном приложении — интернет-браузере. Для борьбы с такими методами нападений уже недостаточно классических способов защиты, поскольку системы безопасности должны знать о допустимости той или иной конфигурации информационной системы, а ведь именно это определяется системой CSM.



СЕГОДНЯ, ЧТОБЫ ОБМАНУТЬ СРЕДСТВА ЗАЩИТЫ, ЗЛОУМЫШЛЕННИКИ ВСЕ ЧАШЕ ПРИБЕГАЮТ К УСТАНОВКЕ ЛЕГАЛЬНЫХ СЕРВИСОВ НА АТАКУЕМЫЙ КОМПЬЮТЕР...

Какие же задачи должна выполнять система, совместно с CSM управляющая информационной безопасностью? Во-первых, сканировать управляемые системы в поисках вредоносного кода или определять его присутствие по некоторым внешним признакам. Во-вторых, автоматически удалять или блокировать вредоносные программы и предотвращать их повторное проникновение в систему. В-третьих, восстанавливать систему после сбоя, вызванного атакой или неудачной защитой от нее, а также собирать и публиковать статистику. Другими словами, в комплексной системе должны

присутствовать такие компоненты, как сканер вредоносного ПО, мониторинг и блокировка нелегальных программ, контроль доступа к информационной системе, программа установки обновлений, модуль восстановления работоспособности программ и система отчетности. Один из примеров подобного программного обеспечения — решение компании LANDesk — Security Suite. Оно включает систему управления обновлениями, модуль защиты от шпионского и рекламного ПО, анализатор угроз безопасности, систему обнаружения и блокирования несанкционированных приложений,



[OC Windows обзаведется онлайн-новым сервисом оптимизации]

Microsoft приступила к тестированию интернет-сервиса по автоматической настройке производительности операционной системы Windows и ее безопасности. Сейчас предварительная версия службы Windows OneCare проходит внутреннее тестирование в Microsoft. С ее помощью пользователи Windows XP Service Pack 2 смогут загружать и устанавливать обновления антивирусных баз и средств защиты от шпионского ПО, резервировать данные и оптимизировать быстродействие. Подписчики Windows OneCare смогут настраивать систему на автоматическую работу. Например, в заданное время компьютер сможет самостоятельно выполнять дефрагментацию, восстановление данных и очистку жестких дисков от ненужных файлов. Полномасштабные испытания Windows OneCare начнутся в конце этого года.

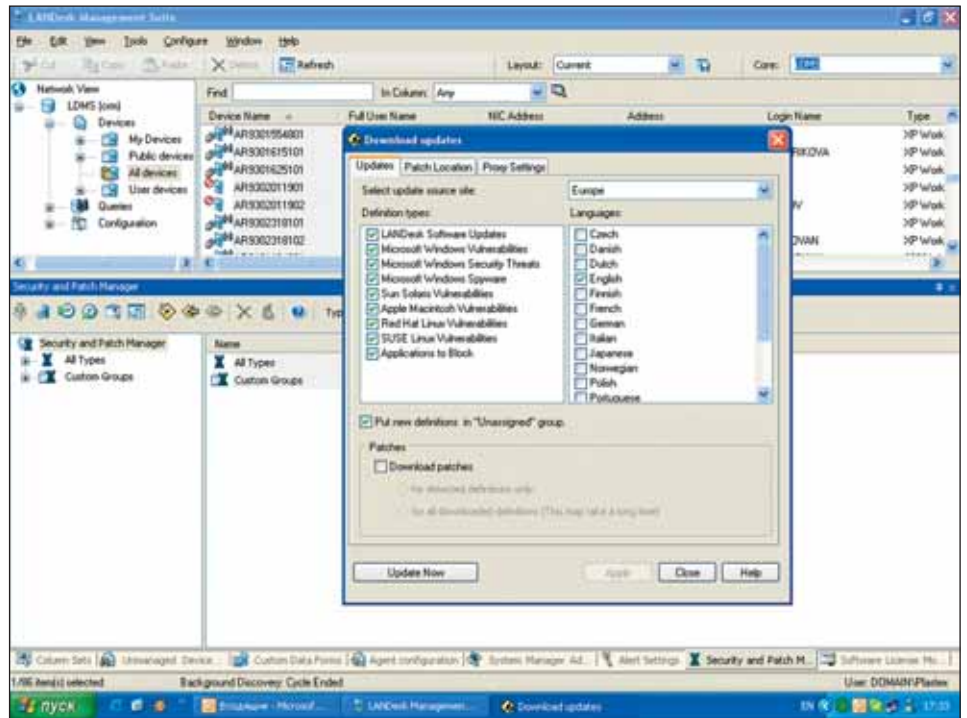
[IBM усиливает безопасность обмена бизнес-информацией]

Корпорация IBM разработала новую платформу для безопасного обмена данными через Интернет. ПО Tivoli Federated Identity Manager (TFIM) представляет собой единую систему доступа к корпоративному portalу для служащих компании, ее клиентов и партнеров. Portal открывает доступ к другим ресурсам (включая Интранет), причем, как заявляет IBM, пользователю достаточно пройти процедуру верификации один раз. TFIM совместима с основными стандартами идентификации, включая Liberty, SAML, WS-Federation, WS-Security и WS-Trust.

[Novell: новый уровень защиты Linux]

Компания Novell приобрела фирму Immunix, разрабатывающую решения для обеспечения безопасности Linux-приложений. Самым популярным продуктом этой компании является система AppArmor, обеспечивающая комплексную защиту компьютеров под управлением ОС Linux от деструктивных программ и хакерских атак. Novell планирует продавать ПО AppArmor под брендом Novell AppArmor powered by Immunix.

LANDesk Security Suite включает систему управления обновлениями, модуль защиты от шпионского и рекламного ПО, анализатор угроз безопасности и другие функции



КОМПЛЕКСНАЯ СИСТЕМА БЕЗОПАСНОСТИ ДОЛЖНА ВКЛЮЧАТЬ СКАНЕР ВРЕДНОГО ПО, МОНИТОРИНГ НЕЛЕГАЛЬНЫХ ПРОГРАММ, КОНТРОЛЬ ДОСТУПА И ДР...

модуль для поиска новых дефектов, систему управления доступом, а также модуль собственного обновления. А теперь рассмотрим принципы функционирования каждого из модулей. Система управления обновлениями (Patch Management) предоставляет возможность администратору просмотреть пакеты обновлений, имеющиеся на подготовленных ему компьютерах. Причем Patch Manager определяет не только обновления, установленные с его помощью, но и те, что могли быть установлены пользователем самостоятельно. Это позволяет удалить те обновления, которые признаны ненужными или даже опасными. Поддерживается работа как с Windows, так и Linux (Red Hat, Novell SUSE) и Mac OS. Одновременно Patch Manager предоставляет возможности по управлению автоматической установкой обновлений, например, определяя конфигурацию по умолчанию, необходимость перезагрузки после установки обновлений и другое поведение системы в процессе установки. Следующий модуль — система защиты от шпионского и рекламного ПО (Anti-Spyware), выпол-

няет все задачи, связанные с распознаванием, блокировкой, лечением и удалением таких программ, как троянские кони, контролеры поведения пользователя и нажатий клавиш на клавиатуре, и других. Данный модуль также восстанавливает файлы, поврежденные в процессе борьбы с вредоносным ПО, и предотвращает повторное заражение вирусами. В свою очередь анализатор угроз безопасности (Security Threat Analyzer) делегирует права администраторов системы. Этот компонент определяет, какие каталоги доступны для монтирования извне и, опять же, проверяет, насколько санкционированы подобные действия. Он следит за тем, какие сетевые сервисы доступны внешнему пользователю и насколько это оправданно. Threat Analyzer проверяет работу контролера домена и межсетевого экрана, доступность гостевого входа, качество паролей, версии операционных систем, уровень безопасности браузеров и многое другое, что может являться признаком успешно завершенной атаки. Система обнаружения и блокирования несанкционированных приложений (Application

Пакет LANDesk Security Suite может быть установлен самостоятельно или интегрирован в систему управления LANDesk Management Suite



Blocker) анализирует, какие приложения могут вести себя подозрительно и в чем именно это выражается, если вирус все-таки проник в систему и начал активно размножаться. Кроме того, он определяет и блокирует запуск приложений, которые не разрешены политикой безопасности, не являются корпоративным стандартом или просто уменьшают защищенность или производительность вычислительной системы.

Модуль для поиска новых дефектов (User-defined Vulnerabilities) и система управления доступом (Connection Control Manager) обеспечивают контроль доступа сетевых приложений к ресурсам компьютера. В частности, этот компонент ограничивает доступ по сети к таким устройствам, как шина USB, модемы, различные съемные накопители, параллельные и последовательные порты и беспроводные устройства. Он же контролирует, насколько разрешено то или иное сетевое подключение, и в случае нарушения политики безопасности поднимает тревогу. И наконец, модуль собственного обновления

LANDesk Update занимается обновлениями различной информации, связанной с работой Security Suite, например устанавливает обновления всех компонентов, входящих в пакет, изменяет правила их работы, а также определяет правила обновления приложений. Различают четыре типа обновлений: ядро (Core), консоль (Console), веб-консоль (WebConsole) и клиент (Client). Каждый из них принадлежит к соответствующим элементам самого пакета Security Suite. С помощью этого компонента система может постепенно развиваться и нарастать на отражение новых угроз. В целом пакет LANDesk Security Suite предлагает практически полный набор функций, которыми должна обладать система управления информационной безопасностью. Интересно, что указанный пакет программ может быть установлен самостоятельно или интегрирован в систему управления LANDesk Management Suite. В последнем случае средствами пакета можно обеспечить полный контроль над корпоративной системой и ее безопасностью.



Symantec заботится о безопасности смартфонов

Компания Symantec представила программное решение для защиты Symbian-телефонов от вирусов.

В состав пакета Symantec Mobile Security 4.0, предназначенного для защиты мобильных телефонов под управлением ОС Symbian, вошли антивирусная программа и брандмауэр. Новый продукт Symantec ориентирован на бизнес-пользователей.

Стоимость двухлетней лицензии на данный пакет составляет \$44,95.



McAfee: активизация хакеров

Специалисты компании McAfee отмечают рост активности всех видов онлайн-угроз в I квартале этого года.

В первой четверти 2005 года исследователи McAfee зафиксировали более тысячи хакерских атак с использованием новых методов взлома программного обеспечения. Это примерно на 6% больше по сравнению с аналогичным периодом прошлого года. Всего же было зафиксировано более 200 тыс. случаев взлома.

С начала этого года доля почтовых червей в общем количестве вирусов, как и в прошлом году, сократилась. В большинстве случаев пользователи попадали на крючок таких вредоносных программ, как Bagle, Netsky и MyDoom.

Что касается шпионских программ, в I квартале их число также возросло: из 5 млн пользователей McAfee почти 1,5 млн обнаружили на своих ПК в среднем три различных типа программ-шпионов.

Атаки фишеров тоже заметно участились – по данным McAfee, ежемесячный рост составил 25%.