тельности, не заставляя сотрудников отвлекаться на обработку документов.

В результате использования on-line услуги по автоматизированной обработке документов в ЗАО «Руссо Транс» отмечают существенное уменьшение числа ошибок и многократное повышение производительности труда сотрудников.

Таким образом, on-line сервис по распознаванию документов будет полезен всем компаниям, которые имеют большой поток типовых документов и хотят освободить своих сотрудников от ручного введения информации в компьютер, и одновременно сократить число ошибок, при этом минимизировав расход на обработку документов.

Затейчук Елена Николаевна *– руководитель направления компании Техкомпас.*
Контактный телефон 8(905)774-62-04.

IBM Tivoli Endpoint Manager for Security and Compliance

Компания IBM

Компания IBM предоставляет инструмент Security and Compliance Analytics (SCA), являющийся Web-приложением платформы Tivoli® Endpoint Manager, предназначенной для оценки рисков и обеспечения безопасности ИТ-инфраструктуры. SCA включает библиотеки и инструменты технического контроля, которые позволяют непрерывно в автоматическом режиме обнаруживать и исправлять ошибки, поддерживать конфигурацию ИТ-системы в работоспособном состоянии.

Ключевые слова: реальное время, безопасность, ИТ-системы, облачные технологии, антивирусная защита.

Сегодня организациям и предприятиям для развития бизнеса необходимо внедрение новых ИТ-сервисов. При этом часто задача требует решения в рамках сильно ограниченного бюджета. Многие организации отдают предпочтение внедрению облачных моделей ИТ-сервисов, чтобы получить все преимущества от их использования, включая уменьшение затрат и перевод расходов из разряда капитальных в операционные, а также масштабируемость, гибкость и эффективное использование человеческих и технологических ресурсов.

Однако облака могут представлять потенциальные риски для безопасности и конфиденциальности бизнеса. Эти проблемы являются основной причиной замедления темпов внедрения облачных технологий в промышленности и крупных организациях. Защита высоко виртуализированных сред от целевых атак и угроз, обеспечение безопасной совместной работы пользователей и защиты данных (изоляция, совместное использование), недостача прямого контроля параметров безопасности и конфиденциальности являются основными растущими проблемами безопасности облаков.

Пакет Tivoli Endpoint Manager for Security and Compliance от IBM призван гарантировать безопасность конечных точек всей ИТ-инфраструктуры организации. Он помогает защитить устройства и предоставить регулирующим органам доказательства того, что все стандарты безопасности соблюдаются. Это простое в управлении и развертывании решение обеспечивает высокий уровень защищенности в среде с большим числом разнообразных устройств: от серверов до настольных ПК. Данное решение поддерживает ноутбуки, работающие через Internet-соединение, и специализированные устройства, такие как кассовые терминалы (POS), банкоматы и киоски самообслуживания.

Это решение способствует уменьшению стоимости и сложности управления ИТ-средой, мало влияет на функционирование самих устройств, обеспечивает повышение производительности труда и более комфортные условия работы пользователей.

Функций безопасности

Функции управления исправлениями обеспечивают широкие возможности по распространению патчей для Microsoft Windows, UNIX, Linux и Mac OS, а также для Adobe, Mozilla, Apple, Java и других приложений среди распределенных устройств независимо от их местонахождения, типа соединения или состояния. Один сервер управления исправлениями способен поддерживать до 250 тыс. устройств, сокращая время установки исправлений без ущерба для функциональности устройств даже по сети с низкой пропускной способностью или территориально распределенной сети. Отчеты, составляемые в режиме РВ, содержат информацию о том, когда и кем были развернуты исправления, а также автоматическое подтверждение того, что исправления установлены. Таким образом, формируется полное решение для развертывания исправлений с обратной связью.

Функции управления параметрами безопасности представляют собой обширную библиотеку технических элементов управления, которые помогают соблюдать требования по безопасности, определяя и исправляя параметры настройки безопасности системы. Библиотеки поддерживают непрерывное соблюдение основных правил безопасности, обеспечивают сигнализацию, восстановление и подтверждение восстановления не соответствующих правилам безопасности устройств. Они также гарантируют проверку всех конечных точек ИТ-инфраструктуры в режиме РВ. Эта функция доставляет полезную информа-

цию о состоянии и степени безопасности устройств независимо от их местонахождения, операционной системы, типа соединения (включая компьютеры, подсоединенные к кабельной сети и периодически подключаемые ноутбуки), а также об установленных на них приложениях.

Средства управления уязвимостями позволяют обнаруживать, оценивать и устранять уязвимости, прежде чем возникнет угроза безопасности системы. Они оценивают системы в соответствии со стандартными определениями уязвимостей, написанными на языке Open Source Security Language (OVAL). При этом в режиме РВ составляются отчеты о неудовлетворительных политиках обеспечения безопасности. Результатом становится улучшенный контроль и полная интеграция на каждом шаге всего процесса: от обнаружения и оценки угроз до их устранения и формирования отчетов.

ИТ-персонал может выявлять и устранять известные уязвимости с помощью автоматических процедур или вручную по всем конечным точкам ИТ-инфраструктуры. Применяя единый инструмент для обнаружения и устранения уязвимостей, администраторы могут повысить скорость и точность, сократив время развертывания исправлений и обновлений ПО. Администраторы могут также распространить управление безопасностью на мобильные устройства, подключенные или неподключенные к сети, настроив сигнализацию для быстрого выявления устройств-нарушителей и их восстановления или удаления.

Средство обнаружения ресурсов предоставляет готовую динамическую ситуационную информацию об изменении условий в инфраструктуре. Возможность частого сканирования всей корпоративной сети обеспечивает полную прозрачность и контроль, помогая гарантировать быстрое выявление с минимальной нагрузкой на сеть всех компьютеров и других IP-адресуемых виртуальных машин, а также сетевых и периферийных устройств, таких как принтеры, сканеры, маршрутизаторы и коммутаторы. Эта функция помогает следить за всеми конечными точками ИТ-инфраструктуры предприятия, включая ноутбуки за пределами корпоративной сети.

Функция управления средствами безопасности от разных поставщиков предоставляет администраторам возможность централизованного управления сторонними клиентскими решениями безопасности от таких поставщиков, как Computer Associates, McAfee, Sophos, Symantec и Trend Micro. Благодаря такому централизо-ванному управлению организации могут повысить масштабируемость, быстродействие и надежность системы защиты. Решение осуществляет контроль состояния устройств, гарантируя постоянную работу клиентов защиты конечных точек и своевременное обновление антивирусных баз. Проверка с обратной связью, в том числе проверка отключенных от сети устройств через Internet, гарантирует, что установка обновлений и других изменений будет выполнена

Автоматический карантин. ПО автоматически оценивает устройства на наличие необходимых настроек для соблюдения правил безопасности и в случае выявления несоответствия может поместить устройство в сетевой карантин. Сервер Tivoli Endpoint Manager получит доступ к такому устройству в целях управления, но всем остальным доступ будет перекрыт.

Семейство Tivoli Endpoint Manager

За всеми функциями Tivoli Endpoint Manager стоит уникальный подход единой инфраструктуры BigFix, при котором принятие решений распределено между устройствами, что обеспечивает преимущества для всего семейства решений со следующими возможностями.

• *Интеллектуальный агент* размещается в каждой конечной точке ИТ-инфраструктуры. Он выполняет несколько функций, включая непрерывную самооценку и контроль, но при этом оказывает минимальное влияние на производительность системы. В отличие от традиционной архитектуры «клиент – сервер», когда все указания поступают из центра управления, агент самостоятельно принимает решения, отправляя сообщения на центральный сервер и извлекая исправления, конфигурации и другую информацию, необходимую для реализации соответствующей стратегии. В результате управляющему серверу всегда известно о ситуации с соблюдением нормативных требований и изменениях состояния устройств, что позволяет быстро составлять актуальные отчеты по нормативно-правовому соответствию.

• *Отчетность*. Единая, унифицированная консоль, встроенная в Tivoli Endpoint Manager, обеспечивает полную информацию, в том числе непрерывную отчетность в режиме РВ и анализ, выполняемый интеллектуальными агентами в конечных точках ИТ-инфраструктуры организации.

• *Возможности коммуникации*. Масштабируемая и легкая архитектура Tivoli Endpoint Manager позволяет любому агенту настроиться на работу в качестве связующего звена между другими агентами и консолью. Такая функция связи позволяет использовать существующие серверы или рабочие станции для распространения пакетов ПО по сети, уменьшая потребность в серверах.

• *IBM Fixlet-сообщения*. Fixlet Relevance Language – это командный язык, который позволяет заказчикам, бизнес-партнерам и разработчикам создавать настраиваемые стратегии и службы для устройств, управляемых посредством Tivoli Endpoint Manager.

Tivoli Endpoint Manager for Security and Compliance является частью всеобъемлющего семейства решений IBM для обеспечения безопасности, помогает справляться с проблемами безопасности в масштабах всей организации.

Http://www.ibm.com