COMPUTERWORLD РОССИЯ
Международный компьютерный еженедельник ■ www.computerworld.ru 24 июля 2001 ■ №26-27 (283-284) ■ стр. 16

Береженого «Дозор» бережет

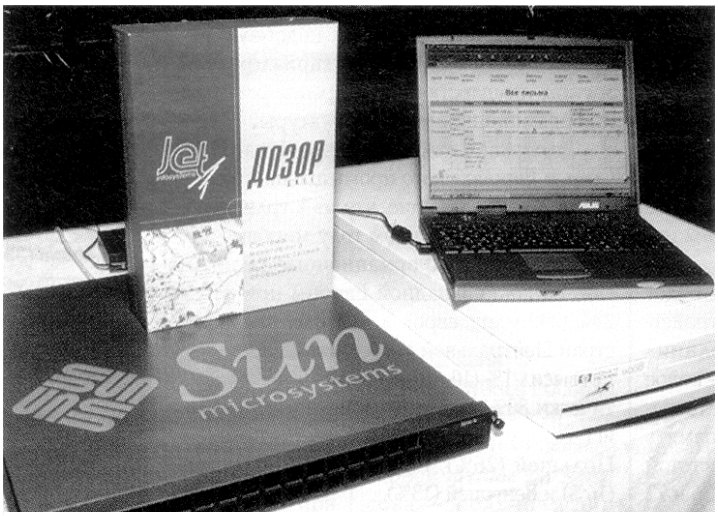
Проблемы безопасности систем корпоративной электронной почты

Игорь Лукьяненко

Электронная почта — это и благо, и немалая потенциальная опасность для компаний. Вопросам безопасного и эффективного использования корпоративной электронной почты был посвящен семинар, который провела для своих клиентов компания «Инфосистемы Джет».

По заверению Сергея Кашинского, начальника технического центра «Инфосистемы Джет», не организованная должным образом система контроля за использованием электронной почты таит в себе массу опасностей: она может стать каналом утечки конфиденциальной информации, сбора компрометирующих данных или входными воротами для вирусов и внешних атак на информационную систему предприятия и т. д. Опасность некоторых из этих факторов уже оценена российскими компаниями, с другими им еще предстоит столкнуться. Например, при разбирательстве дел в американских судах электронная переписка может быть использована в процессе дознания.

Многие, если не все проблемы безопасного использования корпоративной электронной почты можно решить с помощью разных систем мониторинга и контроля, в достаточном количестве предлагаемых на рынке. Но, по мнению Кашинского, наиболее полную защиту от большинства рисков предоставляет система мониторинга и архивирования электронной почты (СМАП) «Дозор-Джет», разработанная в компании «Инфосистемы Джет». Система способна осуществлять мониторинг всех входящих и исходящих сообщений, а также внутренней корреспонденции. Анализ проводится, при опоре на набор правил, которые из большого списка выбирает администратор сети клиента. Ключевым отличием «Дозор-Джет» от других подобных систем ее создатели считают способность с одинаковой эффективностью подвергать анализу все составляющие электронного письма: атрибуты конверта, заголовки и тело сообщения и прикрепленные файлы, включая и архивированные данные. В зависимости от выбранных правил и содержания письма меняются и действия «Дозор-Джет». Система может запретить передачу сообщения, отправить его в архив, за регистрировать, пометить или послать администратору уведомление о наличии того или иного нарушения правил. Как утверждают разработчики, «Дозор-



«Дозор-Джет» и поддерживающие его платформы

Джет» практически не снижает пропускной способности систем корпоративной электронной почты. Так, собственные тесты показали, что СМАП производства«Инфосистемы Джет», функционируя на однопроцессорном сервере Sun Netra t1, может обрабатывать без задержки около 70 Мбайт почты в час.

Для организации последующей обработки отложенная корреспонденция помещается в базу данных под управлением СУБД Oracle, где может храниться неограниченное время и подвергаться обработке различными средствами статистики, анализа и генерации отчетов. Функционирует «Дозор-Джет» на двух популярных Unix-платформах — SPARC Solaris и HP-UX. Продукт уже получил сертификат Гостехкомиссии о соответствии заявленным свойствам и требованиям по защите информации от несанкционированного доступа. Получение сертификата должно облегчить внедрение СМАП на предприятиях, обязанных соблюдать специальные требования и рекомендации Гостехкомиссии по технической защите конфиденциальной информации. Стоимость «Дозор-Джет» для клиента будет зависеть от способа внедрения. «Инфосистемы Джет» будут предлагать как коробочное решение, так и полное внедрение, включающее в себя все процедуры: обследование системы клиента, установку СМАП, тестовую эксплуатацию, сбор и анализ статистики, разработку правил анализа почтового потока конкретного клиента, запуск в промышленную эксплуатацию и техническую поддержку. Лицензирование продукта осуществляется по числу почтовых ящиков в организации. При минимальном комплекте, включающем в себя коробку с программой и лицензией на 50 почтовых ящиков, стоимость «Дозор-Джет» составляет около 3 тыс. долл.