Утечки по каталогу

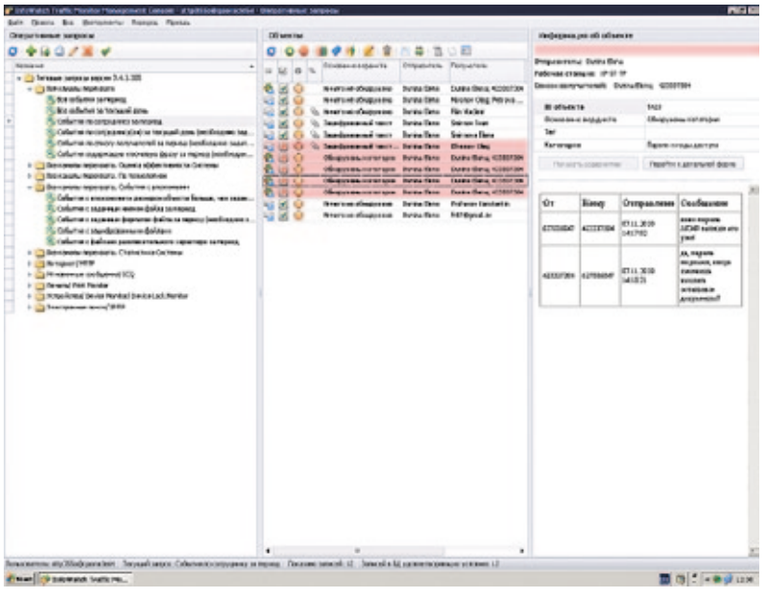
InfoWatch демонстрирует возможности новой версии Traffic Monitor

ВАЛЕРИЙ КОРЖОВ
Computerworld Россия

Компания InfoWatch готовит к выпуску обновленную версию своего флагманского продукта. Среди отличительных черт Traffic Monitor 3.4 MP1 — возможность не только защищать клиента от утечек конфиденциальной информации, но и производить каталогизацию потоков информации, фиксировать маршруты передачи данных и разделять доступ сотрудников к собираемым Traffic Monitor сведениям. Нововведения расширяют область применения продукта — в компании утверждают, что теперь, помимо защиты от утечек (Data Leak Protection, DLP), его можно использовать и для решения других задач.

В новой версии Traffic Monitor в InfoWatch воспользовались лингвистическим ядром собственной разработки, которое базируется на четырех методах анализа информации: лингвистическом, с помощью отпечатков, по шаблонам и контексту. Вердикт выносится с привлечением аппарата нечеткой логики; каждый отдельный параметр имеет свой весовой коэффициент, а результат получается по совокупности факторов. Предусмотрен инструмент автоматического определения контекста документа. Отнеся его к одной из определенных категорий, пользователь может самостоятельно определить категории текстов, указав системе несколько файлов с соответствующими конфиденциальными данными, после чего она проанализирует содержащиеся в них тексты, подобрав ключевые слова и весовые коэффициенты к ним; затем статистику слов и их весовые коэффициенты можно отредактировать, вручную уточнив выводы анализатора. Можно использовать стандартный набор категорий и определять свои.

Именно механизм каталогизации и позволяет решать с помощью продукта новые задачи. В частности, его можно настроить для определения тональности переписки и выявлять отрицательно настроенных сотрудников. Также можно обнаруживать рассылку резюме, чтобы выявить недовольных своей зарплатой. Возможна фильтрация веб-контента, не пускающая пользователей на развлекательные сайты. В этом случае для анализа содержимого сайта используются те же механизмы определения категорий информации, что и в DLP, — это позволяет один раз определить набор категорий для Traffic Monitor, сформулировать для них политику безопасности и следить за ее соблюдением.



TRAFFIC MONITOR ТЕПЕРЬ может не только контролировать, но и блокировать передачу сообщений по электронной почте

Есть и технические нововведения. Например, выполнена интеграция с сервисом каталогов Active Directory, из которых система получает сведения о сотрудниках компании. Кроме того, у продукта появился собственный веб-интерфейс, с его помощью продуктом можно управлять без установки специального программного обеспечения на рабочую станцию. Разработчикам удалось повысить скорость работы шлюзового компонента системы — теперь можно обслуживать потоки данных до 100 Мбайт/с.

Уже в этом году в InfoWatch намерены выпустить еще одну версию своего продукта, четвертую. В ней будет значительно расширено количество поддерживаемых протоколов и каналов коммуникаций. В частности, планируется научить Traffic Monitor контролировать передачу данных посредством Jabber, Yandex Online, «ВКонтакте», LiveJournal, Microsoft Live Messenger, Gmail и Skype. Возможно, это будет сделано путем расширения функциональных возможностей агента, который сейчас устанавливается на все рабочие станции защищаемого предприятия. Сейчас эти агенты защищают от утечек на съемных носителях и с помощью распечатки секретной информации. Однако этот же агент можно использовать и для контроля наиболее сложных коммуникационных протоколов наподобие Skype.

IronBee — межсетевой экран с открытым кодом

Qualys предлагает для облачных сред альтернативу проприетарным механизмам анализа трафика веб-приложений

ДЖОН ДАНН
Techworld.com

По мнению специалистов компании Qualys, существующие межсетевые экраны для веб-приложений не отвечают требованиям, предъявляемым к системам обеспечения безопасности в облаке. В Qualys заявляют, что свое альтернативное видение технологий межсетевых экранов нового поколения они воплотили в собственном с решении с открытым кодом.

Компания Qualys и ее партнер Akamai призывают других участников рынка информационной безопасности к сотрудничеству, предлагая им внести свой вклад в реализацию амбициозного проекта IronBee. Участники проекта намерены создать самый современный механизм анализа HTTP-трафика, который будет обладать необходимой переносимостью при развертывании в разных окружениях и модульностью, позволяющей всем участникам вносить свою собственную лепту в общее дело, не тратя времени на досконального изучение всех деталей.

На первый взгляд отрасли, которая до сих пор делала ставку на развитие частных технологий, брошен серьезный вызов. Как утверждают в Qualys, нынешние проприетарные межсетевые экраны для веб-приложений не только обходятся слишком дорого, но и вынуждены нести на себе непосильный груз обеспечения безопасности всего многообразия существующих СУБД, приложений, унаследованных систем и браузеров.

Перенос этой модели в облако не только снижает уровень безопасности,

Иллюстрация: www.ironbee.com

К НАСТОЯЩЕМУ ВРЕМЕНИ первая версия IronBee готова на 40-50%

но и ограничивает свободу клиентов, у которых могут возникнуть серьезные трудности при переходе на альтернативные системы других поставщиков.

«В условиях дальнейшего распространения облачных технологий и веб-приложений становится очевидным, что ни одна компания не в состоянии справиться со всеми разновидностями атак, которым мы подвергаемся сегодня, — подчеркнул директор Qualys Филипп Курто. — Именно поэтому мы с энтузиазмом приступили к реализации проекта с открытым кодом IronBee, в рамках которого у нас есть возможность использовать при разработке межсетевого экрана для облака опыт всего сообщества. Надеемся, что многообразие применяемых правил поможет нам организовать эффективное противодействие кибератакам».

Qualys вот уже около года ведет предварительные работы, и к настоящему времени первая версия IronBee готова на 40-50%. Ожидается, что пользователи смогут ознакомиться с межсетевым экраном для веб-серверов в третьем или четвертом квартале.