УСПЕХ В ДЕТАЛЯХ

ТЕЛЕКОММУНИКАЦИИ

Создание комплекса средств информационной безопасности (КСИБ) центра обработки данных в ОАО «Уралсвязьинформ»

ОТКРЫТЫЕ ТЕХНОЛОГИИ

Компания Открытые Технологии создала комплекс средств информационной безопасности центра обработки данных в ОАО «Уралсвязьинформ». Построенный комплекс позволяет предотвратить утечку конфиденциальной информации, ее несанкционированную модификацию и уничтожение на различных уровнях: сетевом уровне, уровне серверов, а также на уровне приложений единой системы управления предприятием.

«Высокая ценность информации, хранящейся в центре обработки данных, требует эффективной защиты. Потеря конфиденциальности создает риск раскрытия коммерческой тайны и может нанести ощутимый экономический и репутационный урон. Поэтому компания «Уралсвязьинформ» уделила большое внимание созданию полноценного комплекса средств информационной безопасности ЦОД, использующего самые современные решения в этой области».

Константин Фетисов,
начальник отдела информационной безопасности
Межрегионального филиала информационно-сетевых технологий
ОАО «Уралсвязьинформ»

ЗАКАЗЧИК

ОАО «Уралсвязьинформ» является крупнейшим оператором местной, дальней, мобильной связи и интернет-услуг Уральского региона. Компания работает на территории 8 субъектов РФ общей площадью 1,9 млн кв. км с населением 15,1 млн человек: Курганской, Пермской, Свердловской, Тюменской и Челябинской областей, Коми-Пермяцкого, Ханты-Мансийского и Ямало-Ненецкого автономных округов. По данным на 1 августа 2005 года, ОАО «Уралсвязьинформ» обслуживало 3,5 млн абонентов фиксированной и 2,9 млн абонентов сотовой связи, 500 тыс. пользователей Интернет, занимая 86% рынка услуг местной связи, 80% – дальней связи, более 40% – мобильной связи и интернет-провайдинга. В рейтинге 100 крупнейших компаний Восточной Европы издания Financial Times, опубликованного в июне 2005 года, ОАО «Уралсвязьинформ» занимает 47-е место с капитализацией 1,387 млрд долларов США.

ЗАДАЧА

В рамках проекта создания технической архитектуры, предназначенной для развертывания и эксплуатации Единой системы управления предприятием (ЕСУП) на базе Oracle E-Business Suite, создать комплекс средств информационной безопасности ЦОД, способный минимизировать риски, связанные с утечкой конфиденциальной информации из ЕСУП, несанкционированной ее модификацией или утратой.

РЕШЕНИЕ

В ходе работ по проекту специалистами компании Открытые Технологии был выполнен весь необходимый комплекс работ: техническое проектирование, поставка программно-аппаратного комплекса и пусконаладочные работы. При проектировании и внедрении КСИБ ЦОД были реализованы общие требования по обеспечению безопасности информации ЕСУП, разработанные и принятые управляющей компанией холдинга «Связьинвест» для всех МРК. Перед внедрением комплекса предложенные в техническом проекте решения были протестированы в лаборатории компании Открытые Технологии.

РЕЗУЛЬТАТ

КСИБ ЦОД обеспечивает выполнение данных требований на различных уровнях: сетевом уровне, уровне серверов, а также на уровне приложений OEBS.

В состав созданного КСИБ ЦОД входят:

- подсистема межсетевого экранирования;
- подсистема обнаружения атак;
- подсистема сканирования защищенности;
- подсистема управления КСИБ ЦОД;
- подсистема мониторинга событий ИБ.

Ранее в центре обработки данных, созданном в рамках проекта построения технической архитектуры в ОАО «Уралсвязьинформ», была развернута система мониторинга на базе Micromuse Netcool. При создании КСИБ ЦОД в качестве подсистемы мониторинга событий информационной безопасности была использована специальная конфигурация Netcool for Security Management (NfSM). Решая задачи независимой регистрации и корреляции событий информационной безопасности, NfSM позволяет администраторам безопасности эффективно и быстро выявлять атаки злоумышленников на сервисы ЦОД и оперативно противодействовать их развитию.

ТЕХНОЛОГИИ

При построении КСИБ ЦОД были использованы решения ведущих производителей средств информационной безопасности: Cisco Systems, RSA Security Inc., Internet Security Systems, Application Security Inc. – и возможности обеспечения информационной безопасности, имеющиеся в ПО Oracle и операционной системе HP UX.