ИСТОРИЯ УСПЕХА

Создание единого решения по защите от вирусных и других вредоносных программ в компании «Евросеть»

«Евросеть» является одной из крупнейших компаний, работающих на рынке сотового ритейла и ведущим дилером операторов связи. Основными направлениями деятельности компании являются розничная торговля сотовыми телефонами, цифровыми фотоаппаратами, телефонами DECT, персональным аудио, аксессуарами, подключение к операторам связи и оказание информационных услуг клиентам.

ЗАДАЧИ

Задача – создание единого комплекса для защиты от вирусных и других вредоносных программ центрального, региональных офисов и торговых салонов, в том числе осуществление централизованного администрирования антивирусным ПО.

В компании использовались антивирусные средства различных вендоров, которые работали без централизованного управления и в большинстве случаев не обновлялись, так как инженеры технической поддержки устанавливали антивирусы «на свой вкус», а пользователи имели возможность отключить и не использовать антивирусное средство защиты. В компании не было единой политики использования антивирусных средств, и поддерживать в рабочем состоянии такое разнообразие было невозможно.

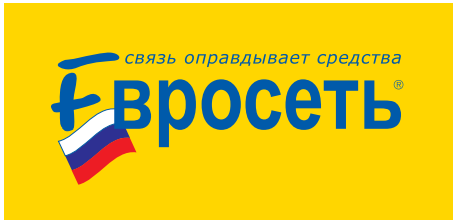
Это приводило к высокой загрузке ИТ-департамента и Call-центра компании при вирусных атаках. Call-центр в период вирусных эпидемий с трудом справлялся со шквалом вызовов от сотрудников, обращающихся по проблемам, связанным с вирусной активностью и невозможностью работать с компьютерами.

По данным службы ServiceDesk в 2006 году зафиксировано 5 критических инцидентов, в 2007 году – 1 критический инцидент. За 2007 год было зафиксировано 2333 инцидента по всей компании, из них 114 с высоким приоритетом.

Устранение критических инцидентов в регионах занимало 2-3 дня, что приводило к сбоям в работе бизнес-подразделений, в том числе к простоям торговых салонов и существенной потере рабочего времени сотрудников компании.

По данным службы ServiceDesk потери рабочего времени торговых салонов в августе 2007 года составили 174 часов 20 минут, в сентябре 2007 года – 149 часов 39 минут.

В связи с большим числом рабочих станций и распределенной структурой (филиалы и торговые точки компании «Евросеть» открыты в 14 странах) критически важным требованием явилось централизованное администрирование: своевременное обновление антивирусных баз большого числа рабочих станций и серверов. Главной проблемой, с которой столкнулись сотрудники компании, стали низкоскоростные и непостоянные каналы связи.



В настоящее время компания представлена более 5000 магазинами, расположенными в 12 странах: России, Армении, Белоруссии, Казахстане, Киргизии, Латвии, Литве, Молдавии, Узбекистане, Таджикистане, Украине и Эстонии.

Сегодня группа компаний «Евросеть» насчитывает 18 региональных филиалов с развитой инфраструктурой местного управления.

РЕШЕНИЕ

Решение – создание единой системы для защиты от вирусных и других вредоносных программ центрального, региональных офисов и торговых салонов.

На первом этапе специалисты компании «Евросеть» совместно со специалистами компании «Инфосистемы Джет» провели обследование сети компании, собрали информацию для проведения проектирования и дальнейшего внедрения.

Почему «Инфосистемы Джет»? «Для участия в проекте мы выбрали компанию «Инфосистемы Джет», исходя, прежде всего, из опыта компании в реализации подобных проектов и репутации надежного партнера. С самого начала проекта мы убедились в том, что сотрудничаем со специалистами самой высокой квалификации – экспертами в данной области», – прокомментировал Сергей Андреев, заместитель начальника группы информационной безопасности.

По мнению специалистов, оптимальным решением являлось создание единого антивирусного комплекса на базе решения Symantec Enterprise Edition, так как функционал ПО Symantec наиболее полно отвечал бизнес-требованиям компании «Евросеть». Symantec Enterprise Edition позволяет достаточно просто решить задачи комплексного внедрения и администрирования антивирусных средств в среде компании.

Почему Symantec? «Во-первых, известное имя и быстрота реакции вендора на распространение неизвестных вирусов для снижения потерь от day-zero атак. Во-вторых, решение, которое обеспечивает прозрачность в работе конечных пользователей: они не отвлекаются на сообщения об уничтоженных вирусах. Антивирус защищает компьютеры без вмешательства пользователей и своевременно обновляться. Все эти факторы, безусловно, позитивно сказываются на бизнесе компании в целом», – прокомментировал Алексей Медведев, начальник группы информационной безопасности.

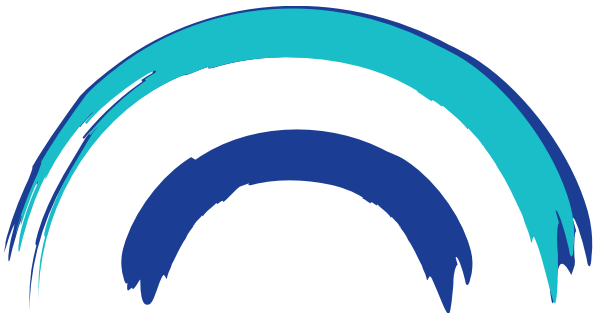
Проектирование, внедрение и поставка ПО осуществляла компанией «Инфосистемы Джет», авторизованным партнером Symantec.

Специалисты компании «Инфосистемы Джет» разработали решение, которое основывается на двух компонентах: компоненте управления средствами антивирусной защиты и компоненте защиты рабочих мест пользователей.

В основе компонента управления средствами антивирусной защиты лежат два сервера управления антивирусным ПО – основной и вторичный. Основной антивирусный сервер через Интернет получает актуальные обновления баз с Symantec Security Response. Вторичный антивирусный сервер выполняет функции по управлению антивирусным программным обеспечением на рабочих станциях пользователей и защищаемых серверах.

Вторичные серверы были установлены в каждом региональном офисе для получения антивирусных баз с основного сервера Головного офиса, а также выполнения обновления антивирусных баз клиентских рабочих мест и файловых серверов.

Кроме того, инженеры компании «Инфосистемы Джет» предусмотрели приложение Reporting Server (сервер отчетов) на основном сервере Головного офиса для возможности получения отчетов по событиям безопасности антивирусной защиты. На вторичных серверах выполняется приложение Reporting Agent (агент сервера отчетов). Агенты пересылают информацию о клиентах Symantec AntiVirus Client на сервер отчетов (Reporting Server), который сохраняет информацию в базу.



Технические компоненты решения:

Внедренный продукт – Symantec Enterprise Edition

Операционная система – Windows 2000/XP

Количество лицензий – 8026

Тип контракта – Gold Maint

Компонент защиты рабочих мест пользователей был разработан из антивирусного ПО, размещаемого на рабочих местах пользователей и взаимодействующего с вторичными серверами.

В рамках проекта эксперты компании «Инфосистемы Джет» разработали регламент антивирусной защиты, который определяет порядок, механизм организации и контроль состояния системы антивирусной защиты «Евросеть» на основе продуктов Symantec.

В результате в компании «Евросеть» была создана система эшелонированной антивирусной защиты на базе технологий компании Symantec.

В настоящее время описанное решение полностью интегрировано в ИТ-структуру компании «Евросеть». При внедрении решения был заключен контракт на сервисную поддержку.

РЕЗУЛЬТАТЫ

В результате проекта создана единая система защиты от вирусных и других вредоносных программ на базе Symantec Enterprise Edition, преимущества которой определяются:

- сокращением простоев торговых салонов, связанных с вирусной активностью;
- сокращением потери рабочего времени;
- прозрачностью взаимодействия с антивирусным ПО для пользователей и интуитивно-понятным интерфейсом для администраторов;
- централизованным управлением;
- своевременным обновлением антивирусных баз;
- оперативной реакцией на очаги вирусных заражений.

«Созданная гибкая система защиты от вирусных и других вредоносных программ с возможностью централизованного управления значительно увеличила эффективность работы конечных пользователей, а также упростила и снизила затраты на администрирование антивирусных средств», – добавил Евгений Акимов, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет».

127015 Россия, г. Москва,
ул. Б. Новодмитровская, д. 14, стр.1
Телефон: +7 (495) 411-7601
Факс: +7 (495) 411-7602
info@jet.msk.su
www.jet.msk.su

О ЦЕНТРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ»

Центр информационной безопасности на сегодняшний день самое крупное подразделение, занимающееся информационной безопасностью, среди всех российских системных интеграторов. В Центре работает более 130 высококвалифицированных специалистов

Компания «Инфосистемы Джет» работает на рынке информационной безопасности с 1996 года и выполняет полный цикл работ по защите корпоративных систем любого масштаба и сложности – от обследования и анализа рисков до внедрения и сопровождения средств и систем информационной безопасности.

Благодаря наличию широкого спектра решений и услуг, сертифицированных специалистов и богатому опыту, а также четко организованной работе проектного офиса Центру доверяют проекты крупные компании, в том числе и транснационального масштаба, с численностью сотрудников в десятки тысяч человек.