McAfee
Protect what you value

КОНКРЕТНЫЙ ПРИМЕР

Mainova AG

Профиль клиента

Экологически чистые источники энергии: электричество, природный газ, отопление и водоснабжение.

Отрасль

Государственный сектор

ИТ-среда

Штат сотрудников Mainova AG составляет 3 000 человек. Сеть охватывает 80 зданий, 2 центра данных и около 300 серверов.

Проблемы

Компании Mainova требовалась масштабируемая система обнаружения и предотвращения вторжений, распространяющаяся на всю сеть и рассчитанная на 60 000 посещений ежедневно.

Решение McAfee

McAfee Network Security Platform I-2600

Результаты

- Полная защита и снижение эксплуатационных расходов, мониторинг решения для обнаружения и предотвращения вторжений осуществляется лишь тремя сотрудниками
- Новая система полностью готова к работе в течение трех недель после установки
- Упрощенное, централизованное администрирование конфигурации и правил обработки угроз
- Точное определение и блокирование угроз в реальном времени
- Полная прозрачность мониторинга сетевого трафика

Поставщик электроэнергии Mainova AG (Франкфурт) доверил сетевую безопасность McAfee

Компания Mainova AG, образованная в результате слияния Stadtwerke Frankfurt am Main GmbH и Maingas AG в 1998 г., обеспечивает регион Рейна-Майна надежными поставками экологически чистых источников энергии: электричества, природного газа, отопления и водоснабжения. Организация разрабатывает инновационные стратегии поставок, предоставляет своим клиентам рекомендации по экономии энергии и эксплуатирует ультрасовременные электростанции.

Крайне рассредоточенная сеть

ИТ-отдел Mainova AG обслуживает такие организации, как Stadtwerke Frankfurt am Main Holding GmbH, VGF (транспортное ведомство Франкфурта) и BBF (ведомство, курирующее работу плавательных бассейнов). В обязанности отдела входит обслуживание всей сети, элементы которой расположены в разных зданиях. Одной из важнейших проблем является сетевая безопасность при интерактивном обслуживании клиентов. Таким образом, задачей ИТ-отдела Mainova AG является защита всего трафика электронной почты и взаимодействия с клиентами в Интернете. Стратегия сетевой безопасности охватывает веб-сайты холдинговой компании Stadtwerke и транспортной компании, обслуживающей район Майна, а также все сопутствующие услуги. К ним относятся онлайн-формы, информационные брошюры, доступные для загрузки, расписание движения транспорта, интерактивная продажа билетов и функции просмотра показаний счетчиков и изменения банковских реквизитов. Частью сети также являются электростанции и различные сложные объекты. Вся сеть доступна 3 000 сотрудников, включает 2 ИТ-центра, сетевую инфраструктуру примерно 80 зданий и около 300 серверов.

В 2004 г. ИТ-отдел Mainova AG столкнулся с необходимостью установить новое решение безопасности для всей сети. Система должна была обеспечить защиту интрасети и сети Интернет, то есть появилась потребность в установке современной системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Прежнее решение, работающее с 2000 г., требовало частого обновления, и договор об обслуживании действующей системы IDS/IPS истекал в ближайшее время. Также возникали трудности с интерпретацией предоставляемых журналов и настройкой параметров системы. Количество посещений сети такого масштаба составляло примерно 60 000 в день, и была поставлена задача устранить все возникающие проблемы. В старой системе персонал ИТ-отдела не имел возможности фильтровать отчеты по журналу, используя собственные критерии, или сортировать и упорядочивать такие отчеты по типу событий. Параметры не позволяли настраивать исключения, например, игнорирование журналов, если они классифицированы как ложная тревога или нерелевантные сообщения.

Выбрано решение на основе устройств

В качестве возможных альтернатив рассматривались следующая версия решения от прежнего поставщика, привлечение внешних ресурсов и предложение McAfee®. Компания Mainova AG установила сервер и организовала 2 теста для оценки обоих решений, использующих внутренние ресурсы. Одним из недостатков привлечения внешних ресурсов было нежелание компании доверить такой важнейший вопрос, как безопасность, сторонней компании. Еще одним аргументом против привлечения внешних ресурсов стала предложенная стоимость, которая значительно превышала расходы по приобретению решения McAfee и ежегодные выплаты за поддержку. После проведения анализа результатов тестов было принято решение внедрить решение на основе устройств, предложенное McAfee.

Решение, разработанное для Mainova AG, основано на двух устройствах с датчиками McAfee Network Security Platform I-2600 и McAfee Network Security Manager. McAfee Network Security Platform I-2600 - это мощное и гибкое решение на основе устройств с датчиками для линий передач корпоративных сетей. Система позволяет компаниям выполнить экономичную интеграцию системы IPS в сети, состоящей из множества точек. Предохранительный щит, использующий запатентованные алгоритмы обнаружения, защищает ресурсы и инфраструктуру сети от целого ряда известных вирусов и атак нулевого дня и «отказ от обслуживания». Система McAfee Network Security Platform I-1600 предлагает богатый набор интегрированных функций управления безопасностью. Таким образом, система значительно упрощает и ускоряет выполнение сложных задач, которые встречаются в старых системах IDS, связанных с администрированием конфигурации и правил, обработкой угроз и обеспечением приемлемого уровня защиты. Новая система IPS работает с использованием запатентованных алгоритмов, обеспечивающих точное и полное определение и отражение угроз в реальном времени. Устройства McAfee развертываются в различных критических точках корпоративной сети и функционируют как датчики, передающие информацию на главный сервер управления и получающие обновления с этого сервера.

Простота интеграции, быстрое решение проблем

Компания McAfee выполнила интеграцию решения для Mainova AG за два дня (или 16 человеко-часов). Еще половину рабочего дня заняла настройка необходимых параметров. Для поиска указаний по эффективной настройке параметров был изучен том журнала практического теста. Решение безопасности было запущено после двухнедельного курса подготовки администрирующего персонала и окончательной настройки параметров. Высочайшая эффективность решения произвела благоприятное впечатление. Оставалось лишь устранить незначительные проблемы с базой данных MySQL, где были выявлены несоответствия с журналами и настройками в системе управления. Все эти проблемы были оперативно разрешены с использованием интерактивного обучающего портала McAfee KnowledgeBase.

Решение на основе устройств не требует трудоемкой настройки операционной системы и исправлений администрирования для датчиков в многочисленных удаленных точках. Все угрозы точно определяются и блокируются в реальном времени. Новое решение по безопасности существенно экономит время. Мониторинг решения IDS/IPS осуществляется лишь тремя из 160 сотрудников ИТ-отдела Mainova AG. Автоматические обновления сигнатур отличается высокой надежностью. «Основным преимуществом решения McAfee является то, что распространение вирусов по IP-подключениям выявляется очень быстро, и службы обмена сообщениями, такие как Yahoo, можно заблокировать на отдельных рабочих местах», — поясняет Клаус Дитер Хольштайн, глава ИТ-отдела Mainova AG.

Полная защита всей сети

При помощи самонастраивающихся устройств с датчиками, централизованного веб-мониторинга и управления политиками вся сеть Mainova AG полностью защищена и требует низких эксплуатационных расходов. Ключевым преимуществом настраиваемого решения IDS/IPS от McAfee является полная прозрачность мониторинга сетевого трафика. Другой важный фактор — широкие возможности масштабируемости, что приобретает особенное значение для таких крупных организаций, как Mainova AG. Положительный опыт работы также повлиял на решение Mainova AG установить McAfee VirusScan® Enterprise на терминалах. Помимо этого, Mainova AG обсуждает возможность обеспечить защиту отдельных компьютеров при помощи McAfee Host Intrusion Prevention.

ООО «МакАфи РУС»
Адрес: 123317, Россия, Москва
Краснопресненская набережная, д.18, Блок «С»
бизнес центр «Башни на набережной»
4-й этаж
Телефон: +7 (495) 967-7620
Факс: +7 (495) 967-7600
http://www.McAfee.ru

5-cor-mnva-002-0907