Визитка

ВЯЧЕСЛАВ МЕДВЕДЕВ,
ведущий аналитик отдела развития компании «Доктор Веб»

Процедура внедрения антивирусной защиты

Достаточно часто в момент выбора (а иногда уже и в момент закупки) клиенты интересуются рекомендациями по порядку развертывания антивирусной защиты или этапам замены ранее используемого продукта. В этой статье речь пойдет о том, как правильно организовать процесс

Крайне важный момент. К сожалению, в большинстве случаев контакты по вопросам продаж идут с менеджерами, а вопрос тестирования передается системным администраторам. В результате зачастую рождается отчет, приводящий в изумление даже вендора. Неверные названия продуктов, древние версии, указания на отсутствие функционала, который в действительности имеется уже несколько лет, и т.д. Нужно все переделывать, но поезд уже ушел, да и корпоративная честь мешает сознаться в отсутствии нужной квалификации у своих специалистов.

1) Изучение возможностей решения в ходе тестовых установок систем защиты рабочих станций, файловых серверов, почтовых серверов, а также серверов управления антивирусной защитой. Здесь также есть несколько подводных камней. Как ни странно, но довольно часто заказчики не знают, что им нужно. И ладно бы вопрос касался функционала, это было бы понятно. Зачастую затруднения вызывает даже вопрос о списке используемого в организации ПО, что, в свою очередь, не позволяет сформировать предложения по списку поставляемого ПО.

Рисунок 1. Варианты развертывания ПО Dr.Web

Вторая проблема связана с тем, что системные администраторы (которые, как правило, и проводят тестирование) хорошо знают используемые продукты, но (естественно) не знают преимуществ и недостатков продукта тестируемого (но при этом ожидают, что подводные камни в случае закупки продукта будут). Соответственно, рекомендуется согласовать с предполагаемым поставщиком список процедур, которые будут реализовываться с помощью закупаемого продукта, и запросить пошаговые инструкции по данному функционалу или, в случае отсутствия таких инструкций, инструкции по тестированию. Это позволит избежать непроизводительного расхода времени на изучение неочевидных вопросов.

2) Проверка действия политик безопасности, сформированных в соответствии с политикой информационной безопасности компании. В связи с тем, что каждый продукт по-своему реализует необходимый компании функционал (например, позволяет или не позволяет использовать произвольный браузер для управления), как список шагов процедуры, так и ее продолжительность могут отличаться. В обычное время это не критично, но в случае вирусного инцидента может быть дорога каждая секунда.

3) Проверка совместимости ПО Dr.Web и ПО, используемого в компании. Несовместимость ПО встречается нечасто, но не учитывать такую вероятность нельзя. Поэтому данный шаг также является обязательным в ходе тестирования предлагаемого продукта.

4) Уточнение плана развертывания ПО Dr.Web по итогам тестовых установок в соответствии со структурой корпоративной сети компании и графиком работы сотрудников.

а) Уточнение времени развертывания компонентов ПО Dr.Web в условиях локальной сети компании. Достаточно часто в ходе закупки задают вопрос о времени, требуемом для развертывания. Практика показывает, что в подавляющем большинстве случаев продолжительность развертывания зависит исключительно от специалистов компании. Согласно той же практике достаточно выходных для полного перевода компании с одной системы

защиты на другую при количестве станций, приближающемся к тысяче.

б) Выбор типа развертывания ПО Dr.Web на локальных станциях и файловых серверах (политика AD, запуск дистрибутивов локально, сканирование сети на незащищенные станции и пр.). В зависимости от пропускной способности сети, наличия Active Directory, требований по защите филиалов и удаленных сотрудников компания может выбрать самые разные варианты развертывания (см. рис. 1).

в) Выбор порядка и времени развертывания ПО в соответствии со структурой корпоративной сети компании и графиком работы сотрудников. Крайне важно обеспечить непрерывность работы компании во время развертывания системы защиты. По закону подлости именно в момент отсутствия защиты могут произойти самые страшные заражения.

Пример схемы развертывания инсталляции антивируса в сети предприятия представлен на рис. 2.

5) Обучение администраторов безопасности компании приемам работы с ПО.

6) Отработка процедур, связанных с удалением используемого антивирусного ПО и установкой ПО.

Как ни странно, удаление используемого антивируса вызывает очень много вопросов. Заказчики требуют, чтобы устанавливаемый антивирус удалял ранее используемый. К сожалению, в большинстве случаев это невозможно. Система самозащиты антивируса, рассчитанная на противодействие злоумышленникам, препятствует его удалению кем-либо.

а) Выработка мер защиты на период отсутствия антивирусного ПО на элементах сети компании. Как вариант, можно на данный период развернуть проверку всего входящего трафика на шлюзе и запретить использование сменных носителей.

7) Проверка локальной сети (защищаемых станций и серверов) на наличие сервисов, необходимых для развертывания ПО в сети компании. В случае необходимости – корректировка правил файерволов, используемых в сети компании. Этот пункт также вызывает затруднения. Как ни странно, но никакой продукт не может сконденсироваться на защищаемом компьютере из воздуха. В зависимости от выбранного типа развертывания необходимо открыть те или иные порты, включить требуемые сервисы и т.д.

Иногда именно ограничения по используемым портам и сервисам, действующие в компании, служат основанием для выбора типа развертывания.

8) Утверждение плана-графика развертывания в сети компании. Доведение плана-графика до сотрудников компании в части, их касающейся. Сотрудники компании должны знать (в части, их касающейся) о проводимых в компании мероприятиях. Специалисты компании в рамках проводимых мероприятий должны иметь возможность оперативно получить доступ к необходимым компьютерам и помещениям. Зачастую без санкции соответствующего руководителя это невозможно.

Замена антивирусного ПО в сети компании

1) Подготовка необходимого ПО в зависимости от выбранного типа развертывания. Вполне очевидно, что для различных ОС, типов приложений и т.д. используются различные дистрибутивы.

- Установка серверов иерархической сети, узлов кластера, а также, если нужно, необходимой базы данных (см. рис. 3).
- Развертывание системы резервирования серверов Dr.Web (см. рис. 4). Любой сервер может упасть. Но падение антивирусного сервера приводит к прекращению обновлений защищаемых станций. Поэтому резервирование антивирусных серверов является насущно необходимым.
- Настройка групп и политик.

Рисунок 2. План-график развертывания ПО Dr.Web в сети компании

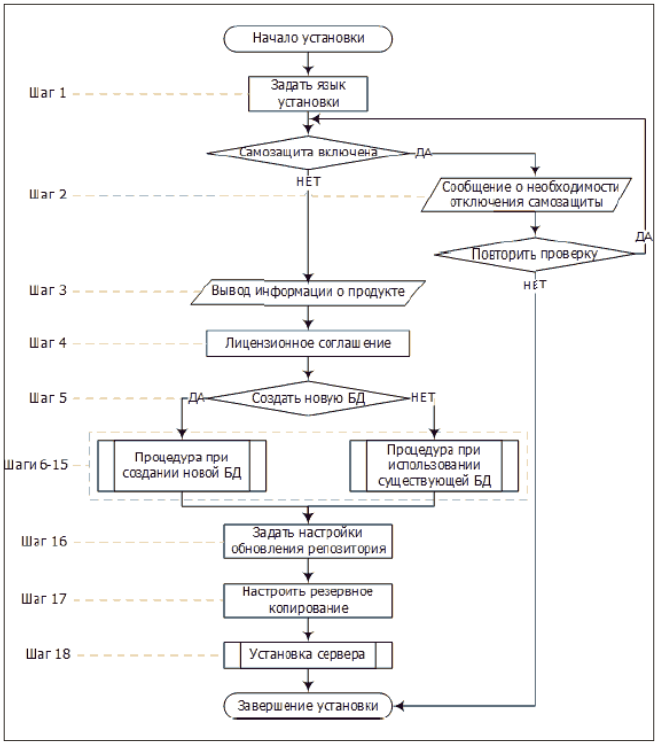
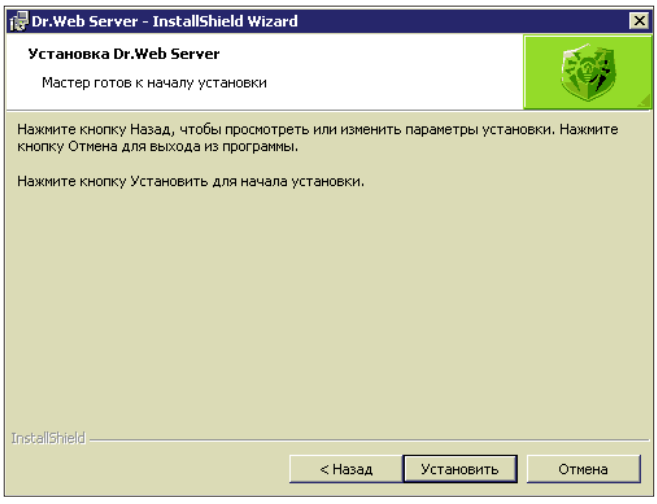


Рисунок 3. Установка серверов



> В случае необходимости – назначение отдельных администраторов группы пользователей и ограничение прав данных администраторов в соответствии с политикой, действующей в компании.
> Проведение требуемых мероприятий в зависимости от выбранной политики развертывания. Например, настройка AD.

2) Сканирование сети компании сетевой утилитой Dr.Web CureNet! на наличие не известных ранее вредоносных программ (см. рис. 5). К сожалению, нельзя гарантировать, что на ПК, на котором предполагается проводить установку, отсутствуют вредоносные программы. Естественно, установка на зараженную машину возможна, но всегда существует шанс, что работающая вредоносная программа имеет функционал, направленный на противодействие установке антивируса. Как минимум это выбьет из графика процесс развертывания защиты, поэтому поверку на наличие вредоносного ПО лучше провести незадолго до установки.

3) Деинсталляция используемых антивирусных продуктов.

4) Развертывание антивирусной сети (см. рис. 6).

> Установка системы защиты рабочих станций и файловых серверов в соответствии с настройками, сделанными на предыдущем этапе.
> Установка системы защиты почтовых серверов, шлюзов сети Интернет.

5) Эксплуатация программного обеспечения в течение тестового периода.

6) Проведение обновлений ПО в соответствии с политикой, действующей в компании.

7) Проведение периодических проверок защищаемых рабочих станций, файловых и почтовых серверов (см. рис. 7).

8) Контроль действий ПО на тестовые воздействия вредоносного ПО.

9) Проверка процедуры взаимодействия с технической поддержкой.

В общем, ничего сложного, если готовиться к любому этапу заранее.

Удачи в развертывании! ADV

Рисунок 4. Развертывание системы резервирования серверов Dr.Web

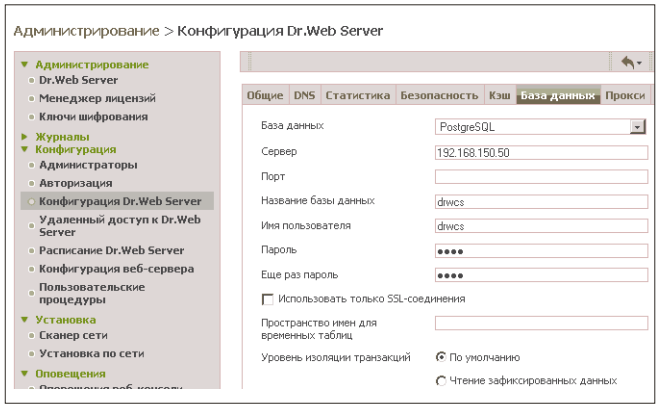


Рисунок 5. Проверка сети компании утилитой Dr.Web CureNet!

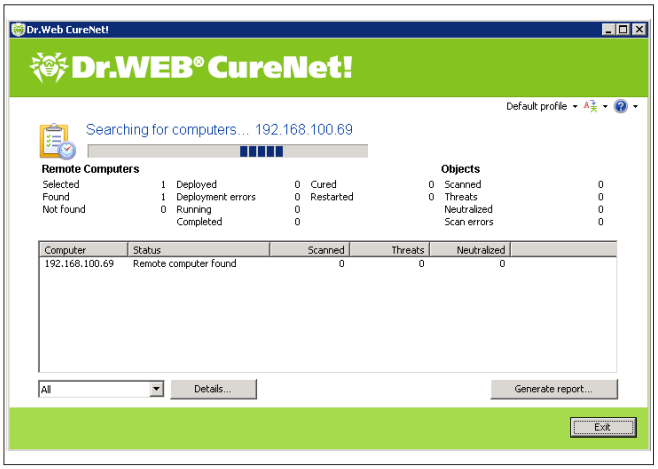


Рисунок 6. Развертывание антивирусной сети Dr.Web Enterprise Security Suite

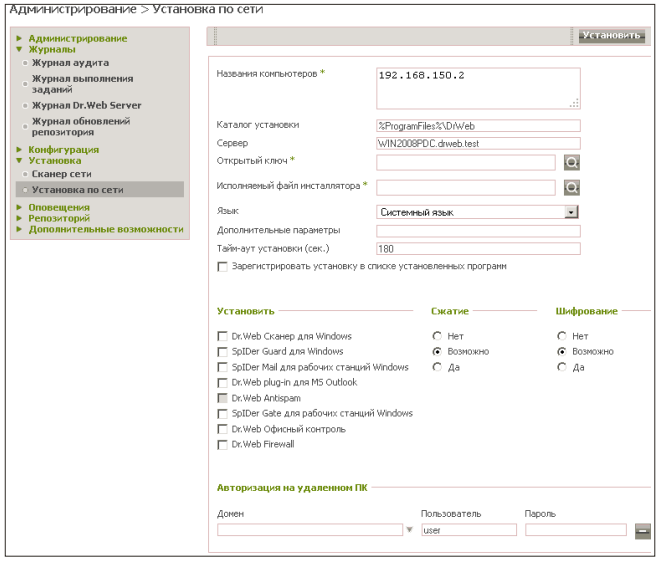


Рисунок 7. Периодическая проверка защищаемых рабочих станций, файловых и почтовых серверов