

SOPHOS Endpoint Security and Control: Взять контроль за безопасностью в свои руки

IT-отделы многих компаний находятся под постоянным прессом, заставляющим их искать новые пути для снижения стоимости IT-систем, нагрузки на службу сервиса и максимизации показателя возврата инвестиций в информационные технологии (ROI). В тоже время вопросы безопасности все чаще беспокоят руководство компаний, по мере внедрения в нашу жизнь компьютеризированных систем, и постоянного повышения стоимости хранимых корпоративных данных. Растущее количество не только вредоносного кода, сколько недопустимого в корпоративных сетях программного обеспечения, такого как ПО для P2P сетей (BitTorrent, Kazaa, Emule и т.д.), персональные интернет-пейджеры (ICQ, AOL IM, Jabber и т.д.), игры и т.д., снижают стабильность работы корпоративных информационных систем и их безопасность. Растущие возможности по беспроводному соединению, позволяют сегодня внедрять в корпоративные сети программы-шпионы, не осуществляя при этом физического соединения. В офисах появляется все больше мобильных компьютеров, каждый из которых часто может стать источником непреднамеренного заражения сети.

НАДЕЖНЫЕ И ПРОСТЫЕ В ЭКСПЛУАТАЦИИ ПРОДУКТЫ SOPHOS ПРИМЕНЯЮТ ДЛЯ СВОЕЙ ЗАЩИТЫ БОЛЕЕ 100 МИЛЛИОНОВ ПОЛЬЗОВАТЕЛЕЙ БОЛЕЕ ЧЕМ В 150 СТРАНАХ МИРА.

Таким образом, IT-специалисты должны иметь в руках мощные инструменты полного real-time контроля за состоянием корпоративной сети и сохранности данных, получать своевременные предупреждения о внештатных ситуациях. Еще несколько лет назад для решения многих проблем с безопасностью было достаточно установить антивирусное программное обеспечение, которое могло бы обновляться без участия специалиста. Но практика применения средств защиты на местах показывает, что сотрудники компаний, часто обладая административными правами на своих компьютерах, просто отключали систему защиты, не уведомляя об этом IT-отдел. В результате дорогостоящая система безопасности не могла эффективно справляться со своими задачами. Серьезной ошибкой многих производителей средств информационной защиты является слабое внимание не только к такому понятию как «защита», но и к такому понятию как «контроль».

Компания Sophos

Компания Sophos уже 20 лет разрабатывает и предлагает решения по защите корпоративных информационных сетей. Sophos не выпускает продуктов для домашних пользователей, прежде всего потому, что в существуют коренные отличия в принципах построения систем защиты для компаний и подобных систем для домашних станций, вот лишь некоторые из них:

Домашний	Корпоративный
Имеет максимальный уровень доступа к ресурсам операционной системы и права локального администратора	Не имеет возможности устанавливать программное обеспечение, не должен иметь возможности отключать защиту, или менять свои права доступа
Все ПО защиты от угроз устанавливается на один компьютер, таким образом требуются решения «все в одном»	ПО защиты распределено в корпоративной сети, и требует адекватной системы управления, учитывающей множественность настроек разных рабочих станций в сети
Использует все доступное программное обеспечение по желанию и возможностям	Обычно запрещены многие приложения, такие как клиенты P2P-сетей, Интернет-пейджеры (ICQ, AOL IM и др.) или компьютерные игры
Обычно используется один компьютер, редко больше	Большое число компьютеров, которые следует группировать для задания им различных политик безопасности и уровней доступа пользователей в группах (например, с использованием Active Directory)

Отличий можно перечислять еще довольно много, однако на данном этапе можно заметить, что производители антивирусного программного обеспечения обычно поделены на два лагеря:

- завоевавшие одобрение со стороны домашних пользователей и небольших компаний сектора СМБ,
- работающие в основном на корпоративном рынке.

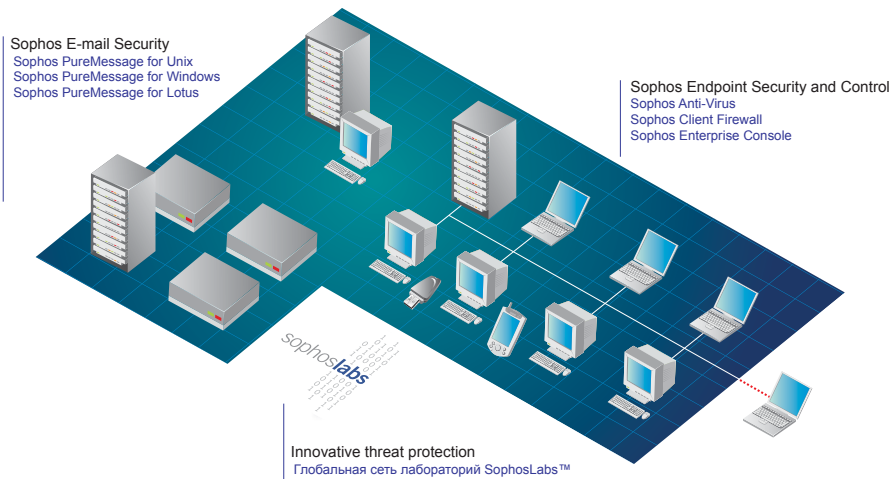
Следует отметить, что такое деление условно, так как многие «домашние» компании сегодня активно переходят в корпоративный сектор, а многие компании второй группы выпускают программное обеспечение для защиты также и домашних пользователей.

Решения Sophos

Все решения Sophos для защиты от информационных угроз (из представленных в России) можно условно разделить на 2 части:

- **Sophos Endpoint Security and Control** – защита рабочих станций и файловых серверов, а также мобильных компьютеров;
- **Sophos E-mail Security** – антиспам и антивирус для защиты почты.

Основным компонентом защиты почты от Sophos является многоплатформенный программный продукт Sophos PureMessage. За счет целого ряда передовых технологий распознавания спама и вирусов, в том числе и автоматического распознавания волн спамовых рассылок, Sophos PureMessage на сегодня является одним из наиболее эффективных западных продуктов в своем классе. Более подробно об этом семействе продуктов можно узнать на сайте компании ДиалогНаука (www.dialognauka.ru).



Стоит отметить, что немаловажным фактором любой системы защиты является ее грамотная и доступная система поддержки и создания обновлений. Здесь Sophos может предложить не только услуги технической поддержки (поддержка на русском языке осуществляется компанией ДиалогНаука), но и глобальной сетью лабораторий и технических центров – Sophos Labs™. Лаборатории Sophos расположены в Австралии, Европе, а также по обоим побережьям Северной Америки, что дает возможность упреждения массовых информационных атак и спамовых рассылок.

В рамках данной статьи мы больше познакомимся с семейством продуктов Sophos Endpoint Security and Control, новая версия которых вышла в июле 2007 года.

Sophos Anti-Virus

Антивирус Sophos сегодня является результатом 20-ти летней совместной работы разработчиков программного продукта и специалистов по информационной безопасности. Одним из коренных отличий данного антивируса является единый агент, который устанавливается на каждой защищаемой рабочей станции. Один агент решает вопросы защиты от всех известных видов информационных угроз, таких как: вирусы, трояны, программы-шпионы, программы-рекламы и другие, кроме того этот же агент используется для связи с системой централизованного управления Sophos Enterprise Console и с системой управления обновлениями Sophos EM Library. Часто в продуктах других компаний программное обеспечение для защиты от вирусов и защиты от программ-шпионов (spyware) представлены в виде независимых модулей, лицензируемых отдельно, что повышает общую стоимость системы защиты и усложняет управление.

Sophos Anti-Virus имеет уже 39 наград известного журнала Virus Bulletin (<http://www.virusbulletin.com>) по состоянию на август 2007 года. Что подчеркивает не только устойчивое качество по поиску и противо-

действию вредоносным кодам, но и проверенная временем надежность продукта на разных операционных системах. Sophos Anti-Virus на данный момент поддерживает 17 различных платформ, включая все версии Windows (антивирус Sophos одним из первых получил сертификат соответствия новой операционной системе Windows Vista), Linux, Mac OS X, HP-UX, IBM AIX, Solaris, Novell Netware и много других.

Многоплатформенность антивирусной защиты Sophos позволяет использовать один продукт с единой системой обновлений на самом разнообразном компьютерном парке, и позволяет повысить качество управления защитой в гетерогенных сетевых средах.

В новой версии Sophos Anti-Virus 7.0 появилась технология поведенческого анализа Sophos HIPS. Уникальность такого проактивного подхода заключается не в анализе кода программ на предмет опасности, а анализе поведения данных программ в специальной безопасной среде. По результатам такого анализа можно устойчиво выявлять новые вирусы еще до того, как их описание попало в базу антивируса. Кроме того, технология Sophos HIPS позволяет противодействовать «таргетированным» атакам, то есть информационным атакам, специально подготовленным для нанесения ущерба только одной – атакуемой – компании. В этом случае глобальная сеть лабораторий сможет выпустить обновление не так быстро, так как не имеет образца кода вредоносной программы, однако вероятность отражения такой атаки с Sophos HIPS (Host Intrusion Prevention System) намного повышается.

Sophos Client Firewall

Уже не первый год в составе продуктов для защиты рабочих станций компания Sophos предлагает не только антивирус, но и брандмауэр – Sophos Client Firewall. Уникальность брандмауэра от Sophos заключается не только в бессмысленном блокировании сетевых портов компьютера, но и анализе сетевой активности программ, установленных на рабочей станции, а также скрытых процессов, имеющих сетевую активность.

Технология сочетания антивируса и брандмауэра по достоинству была оценена уже давно, поэтому такие решения от разных производителей весьма популярны среди домашних пользователей, и теперь приобретают популярность в корпоративных средах.

Основными преимуществами решения Sophos являются:

- централизованное управление брандмауэром через управление политиками безопасности на рабочих станциях;
- режим обучения брандмауэра, в котором производится его автоматическая настройка на специфику сетевой работы в конкретной рабочей группе.

Сочетание этих двух технологий позволяет производить довольно сложную настройку брандмауэра посредством обучения, например, одной рабочей станции в группе, с последующим распространением настроенных правил по всей группе. Данный метод безуслов-

но экономит время на настройку системы, и позволяет создавать правила работы, тонко подстроенные под специфику конкретных рабочих групп.

Sophos Enterprise Console

В данной статье уже несколько раз обращалось внимание на тот факт, что в корпоративных рабочих сетях следует уделять строгое внимание гибкости и простоте управления всей системой защиты. Если администратор не имеет наглядного «real-time» доступа к информации о том, что происходит в корпоративной сети, а также не может оперативно вмешиваться в ее работу при необходимости, то устойчивость такой системы защиты к информационным угрозам сильно ослабнет. Многие обращают внимание на тот факт, что если на рабочих станциях и серверах установлен «хороший» антивирус, то это решает все проблемы с безопасностью. Этот подход давно устарел, так как он отвечает на вопрос «чем защищать», а такие вопросы как: «что защищать» и «как защищать», остаются без ответа.

Хорошим примером в данном случае является требование к системе управления защитой автоматически распознавать подключение к сети новой рабочей станции, гостевой или просто мобильной. Требование не сложное, однако, выполняется оно далеко не всегда. Кроме того, в доменных сетях широко используется технология LDAP, с помощью которой администратор может создавать группы пользователей и назначать им различные права, например, на доступ к общим информационным ресурсам. Однако на практике синхронизация групп пользователей, например, в Active Directory, и групп пользователей в системе управления безопасностью, происходит вручную.

В новой версии консоли управления сетевой безопасностью Sophos Enterprise Console 3.0, компания Sophos постаралась учесть максимальное количество требований к управлению защитой в корпоративных сетях. Если взглянуть на внешний вид консоли, то бросается в глаза ее новый компонент – Dashboard, располагаемый в верхней части экрана. Основным назначением данного компонента является наглядное информирование администратора о состоянии текущей сети. Из данной панели можно узнать о компьютерах, на которых не обновлена антивирусная база, или

компьютерах, которые не соответствуют групповым политикам безопасности, разделить рабочие станции на управляемые с консоли и не управляемые и т.д. Кроме нотификации непосредственно на самой консоли, можно настроить те события, по возникновению которых на специальный электронный адрес будут отсылаться уведомления. При этом такими уведомлениями могут быть не только нотификация о тревожных событиях, неисправностях или заражении, но также и информационные сообщения о подключении новой рабочей станции к сети и т.п.

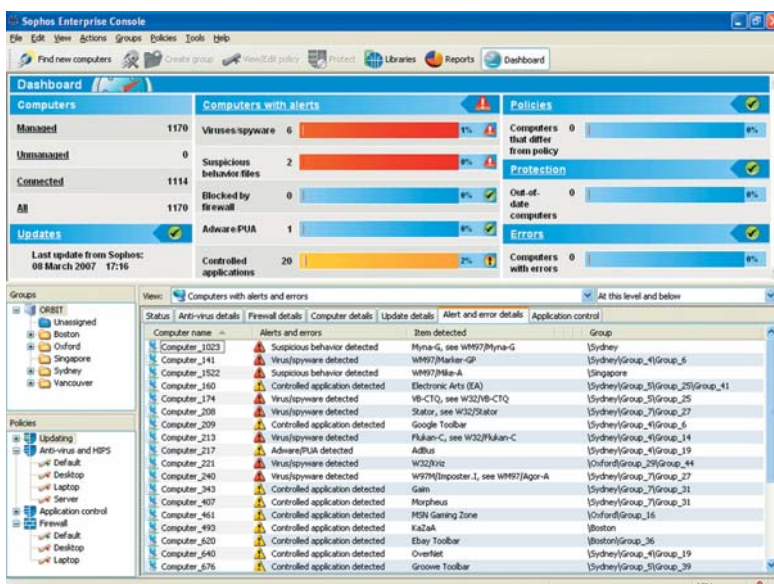
Следующими двумя компонентами консоли, располагаемыми в левой части, являются список групп компьютеров и список политик безопасности (для антивируса, брандмауэра, системы обновлений, и системы слежения за приложениями Sophos Application Control). Отличительной чертой настройки групп компьютеров в консоли является то, что они могут быть созданы как вручную, так и посредством синхронизации с системой Active Directory, для чего следует в одной из корневых групп установить точку привязки.

Настройка политик безопасности производится для всех компонентов агентов, устанавливаемых на рабочих станциях. Таким образом, обеспечивается централизованное управление политиками информационной безопасности с единой консоли. Через установку соответствия между политиками и группами производится присвоение политик безопасности каждой управляемой рабочей станции. Если станция по каким-либо причинам этой политике не соответствует, то в списке компьютеров в группах будет произведена соответствующая нотификация администратора.

Список рабочих станций располагается в средней части консоли, при этом доступна фильтрация компьютеров как по группам, так и по их различным характеристикам, например:

- управляемые или неуправляемые компьютеры;
- компьютеры, на которых не установлен антивирус или другое ПО из комплекта Sophos Endpoint Security;
- компьютеры, не соответствующие установленным политикам безопасности и т.д.

Консоль управления специально спроектирована для управления большим массивом рабочих станций и серверов, работающих под операционными системами Windows, Linux и Mac OS X.



В заключении хотелось бы отметить, что решение Sophos Endpoint Security and Control может быть интегрировано с такими системами как Sophos E-mail Security и Sophos NAC (о котором речь пойдет в следующей статье), создавая тем самым единую среду управления безопасностью всей корпоративной сети. Такой комплексный, многокомпонентный, простой и наглядный механизм противостояния информационным угрозам уже нашел многих почитателей и завоевал немало наград различных изданий. Совокупность многих технологий, таких как Sophos HIPS, Application Control, Client Firewall, Anti-Spam, NAC и других в одном решении дает высочайший уровень защиты, так востребованный сегодня многими крупными и малыми компаниями.