Тема номера
Новости
SQL Server
Exchange & Outlook
Office System
Windows изнутри

Текущий номер
Архив
Об издании

Самое читаемое

Новая система Fujitsu ETERNUS CS800
Оптимизация SQL Server в виртуальной среде
Путеводитель по лабиринту виртуализации
PowerShell Plus 4.0
Начинаем работать с System Center Service Manager 2010
Антивирусная защита: новый этап
Безопасная виртуализация VMware

Ранее в разделе

Диагностика неполадок с помощью Xbootmgr

28/11/2011 №11

«Windows IT Pro» , № 08, 2009

Программы и сценарии

Фильтрация трафика как первый шаг к безопасности сети

Алена Маркова

По данным статистики, при отсутствии гибкой фильтрации доступа к Internet на долю ненужных и опасных сайтов, ежедневно посещаемых сотрудниками, приходится порядка 42% общего трафика, еще 22% занимают ресурсы спорные и только 36% ресурсов могут быть расценены как полезные и имеющие отношение к работе (BrightCloud, 2008, http://www.brightcloud.com/longtail.asp).

Лидерами в списке нежелательных ресурсов являются социальные сети, порталы, выкладывающие контент непристойного содержания, серверы онлайновых игр, а также сайты, генерирующие так называемый «тяжелый» трафик и предлагающие посетителям загружать и просматривать видеоролики и флэш-баннеры.

Потенциальные угрозы, возникающие в результате посещения сотрудниками различных не относящихся к выполняемой ими работе сайтов, помимо нецелевого использования рабочего времени, могут выглядеть как:

- чрезмерная нагрузка на сеть, вызванная неконтролируемым скачиванием сотрудниками объемных файлов из Internet. В случае когда речь идет о постоянном или выделенном подключении с фиксированной скоростью канала от провайдера, просмотр или загрузка пользователями видеофайлов, например с YouTube или файлообменных сетей, негативно скажется на распределении ресурсов сети и загрузке Internet-канала в целом, а также на стоимости нецелевого трафика;
- нерациональное использование ресурсов сети и рабочего времени в результате деятельности любителей онлайновых игр с видео- или голосовыми чатами;
- неконтролируемые удаленные соединения сотрудников с рабочими серверами корпоративных сетей посредством VPN-соединений или утилит, аналогичных Hamachi, сопряженные с риском заражения локальной сети вирусами, потенциально находящимися на удаленном компьютере;
- снижение уровня безопасности корпоративной сети — именно внутренние ресурсы и данные компании часто становятся объектом угроз и рисков при отсутствии полноценного контроля посещаемых сотрудниками сайтов той или иной тематики. По данным Computer Economics, размеры мирового экономического ущерба от различных вирусов могут исчисляться десятками миллиардов долларов в год. Так, например, годовой ущерб, нанесенный вирусом с названием Melissa, оценен в 1,1 млрд. долл. (Computer Economics, 2000).

Зоны рисков

Потенциальными зонами риска распространения вредоносных кодов и фишинговых атак, причинами утечки информации, кражи паролей и других шпионских ухищрений были и остаются порносайты, всем известные социальные сети и блоги, развлекательные порталы и иные подобного рода сайты, где ежедневно инфицируются тысячи новых страниц и появляются новые модификации хорошо известных угроз.

Так, например, в 2008 году пользователи социальной сети «В Контакте» стали жертвами сетевого вирусного «червя», который рассылал с инфицированных машин ссылку на зараженный ресурс другим пользователям сети.

Кроме того, по мнению специалистов WatchGuard Technologies (WatchGuard Technologies, 2009, https://www.watchguard.com/latest/security-predictions.asp), атаки на пользователей будут направлены с привычных и не вызывающих подозрений сайтов, которые незаметно заражаются SQL-инъекциями.

Зараженные сайты могут охватывать широкий спектр интересов, а следовательно, и категорий Internet-ресурсов: от автомобилей, туризма, знакомств, фильмов и музыки до сайтов по трудоустройству, недвижимости и других, на первый взгляд совершенно безобидных сервисов, предлагаемых сегодня Сетью. Находящийся на зараженных сайтах вредоносный код, попадая на один компьютер легкомысленного сотрудника, мгновенно распространяется по локальной сети, нанося компании порой неоценимый ущерб.

Хроника дня

9 Апреля 2012

17:13 В Санкт-Петербурге с помощью мобильного телефона можно оплатить проезд в маршрутке

16:15 «Яндекс.Деньги» – самая популярная система электронных денег у россиян

16:06 «Ростелеком» начала выдачу электронных подписей в Сибири

15:51 Бизнесмен приговорен к 180 часам обязательных работ за комментарий в Интернете

Вся хроника

По статистике большая доля утечек информации приходится именно на действия сотрудников по неосторожности, и только малая часть — на целенаправленно подготовленные злоумышленниками атаки.

Несмотря на эти широко известные факты, по данным исследования Vault, порядка 87% служащих посещают социальные и развлекательные ресурсы на работе, выходя в Internet с подключенных к корпоративной сети рабочих ПК. Причем более 50% делают это как минимум один раз в день, вопреки всем соображениям безопасности, подвергая риску сеть в целом (согласно исследованию Vault.com, 2005).

Необходимо отметить аспект эффективности работы сотрудников: каждые потраченные на прочтение ненужных ресурсов, просмотр фотографий и чтение форумов 5–10 минут в час в конце месяца суммируются в десятки потерянных для компании и оплаченных впустую часов работы.

Механизмы фильтрации трафика

Чтобы обеспечить безопасность и целостность бизнеса, перекрыть каналы возможной утечки информации и повысить производительность работы сотрудников, необходимо управлять потоком Internet-трафика, входящего в локальную сеть. Единственно правильным решением в борьбе со стихийным и неконтролируемым трафиком в любой организации должна стать фильтрация Internet-запросов. Запрещая при помощи настройки фильтров доступ к тем или иным ресурсам, можно не только оптимизировать рабочее время сотрудников, но и легко решить вопросы снижения затрат на нецелевые Internet-ресурсы, а также значительно уменьшить риск инфицирования внутренних ресурсов корпоративной сети.

Большинство компаний давно озабочены поиском и внедрением решений надлежащего уровня, позволяющих минимизировать внешние угрозы и контролировать доступ в Internet. Многие компании-разработчики (как, например, Entensys и др.) активно разрабатывают продукты для Internet-безопасности и фильтрации Internet-ресурсов в сотрудничестве с вендорами — разработчиками систем фильтрации и антивирусных решений, что обеспечивает пользователей комплексным решением современного уровня. Гибкий инструментарий BrightCloud встроен в UserGate Proxy & Firewal (www.entensys.com), что позволяет компаниям малого и среднего бизнеса, государственным структурам, а также некоммерческим и образовательным заведениям регламентировать доступ к различным категориям сайтов.

Американская компания BrightCloud Inc (http://brightcloud.com)является разработчиком механизмов URL-фильтрации по категориям. Ее основная база данных содержит более 450 млн постоянно обновляемых Internet-страниц, сгруппированных в 70 основных категорий сайтов (полный перечень категорий сайтов представлен на http://www.brightcloud.com/masterdburllist.asp), таких, как «Знакомства», «Игры», «Социальные ресурсы», «Покупки», «Путешествия», «Обучение», «Бизнес и экономика», «Internet» и многие другие, включающие рейтинги доверия по каждой категории, а также множество Internet-ресурсов на всех основных мировых языках. Особо стоит отметить расширенную поддержку русскоязычных сайтов.

Именно тематическая категоризация нежелательных ресурсов делает удобной настройку системы фильтрации, поскольку при ее внедрении нет необходимости перечислять и запрещать отдельно каждый нежелательный сайт вручную; достаточно запретить категорию, и все попадающие под данную тематику ресурсы будут автоматически закрыты для посещения сотрудниками. Кроме того, данный подход позволяет отойти от неэффективного деления множества сайтов на так называемые «черные» и «белые» листы, делая политику безопасности более гибкой.

Используя различные правила фильтрации и регулярно анализируя, что же именно загружают из сети сотрудники, можно значительно сократить нецелевой расход трафика и потери рабочего времени (см. экран).

В развитых продуктах также можно настраивать ограничения на загрузку «тяжелых» файлов, например видео или файлов, превышающих определенный размер. В совокупности с разграничением доступа по категориям сайтов это оптимизирует использование сетевых ресурсов и нагрузку на внешние каналы доступа к Internet, избавляет от лишних затрат на трафик и обеспечивает дополнительную безопасность офисных компьютеров внутри периметра сети.

Интегрированные антивирусные модули, в свою очередь, обеспечивают фильтрацию входящего трафика на предмет наличия вирусов, пропуская только безопасный трафик и делая защиту локальной сети всесторонней и комплексной.

Следите за трафиком

Использование Internet-трафика с каждым днем становится все более масштабным, в связи с чем растет актуальность описанных задач по защите сетей от атак, контролю распространения вирусов и несанкционированной сетевой активности пользователей, снижению нерационального использования ресурсов. Потребность в анализе трафика возросла настолько, что решение,

обладающее гибкими механизмами фильтрации, стало жизненно необходимым для множества компаний, использующих Internet.

Алена Маркова (amarkova@ngs.ru)

Комментарии

Логин:

Пароль:

Вход

Для добавления комментариев войдите на сайт