2. Независимый информационно-аналитический центр [Электронный ресурс]. Режим доступа: http://www.anticrimeware.ru/reviews/AVG_Internet_Security_2012

3. Официальный сайт антивируса AVG [Электронный ресурс]. Режим доступа: http://www.avg.com

П.С. Комельских, Федорова А.В. РГППУ
студенты группы КТ-307

«ОБЛАКА» НА ЗАЩИТЕ ДАННЫХ»

Вопрос защиты любой информации всегда оставался и остается актуальным вне зависимости от времени и места. А в современном мире, когда сплошь и рядом компьютерная техника, вопрос защиты от вредоносного и нежелательного программного обеспечения актуален как никогда.

С каждым годом, месяцем и днем появляются все больше новых вирусов, более модифицированных, менее поддающихся «лечению». Когда старые методы поиска и лечения уже не так эффективны, разработчики антивирусных решений ищут новые, все более совершенные технологии защиты от вирусов.

На сегодняшний день существует несколько тенденций, прослеживающихся в разработке антивирусных технологий. Одной из быстро развивающихся разработок являются так называемые облачные технологии, или по-другому – «cloud computing». Это направление отличается революционным, совершенно новым подходом к защите данных.

На протяжении последнего десятилетия, Интернет стремительно вырос как численностью аудитории, так и технологиями. Но злоумышленники не отстают, а даже диктуют свои условия игры в сфере компьютерной безопасности. Например, в последние годы стремительно развиваются и плодятся так называемые «ботнеты»- компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным про-

граммным обеспечением, скрытно установленным и позволяющим злоумышленнику управлять некими действиями с использованием ресурсов зараженного компьютера.

Злоумышленники ищут уязвимости в программных обеспечениях, используют более хитрые вирусные программы, а все для того, чтобы обойти систему защиты и взять управление над ПК пользователя. Эти вирусные программы постоянно видоизменяются и развиваются, и базы сигнатур антивирусных компаний увеличиваются. С этим увеличиваются базы сигнатур и у пользователя на ПК, и затрачивается все больше памяти для хранения и сравнения сигнатур, тем самым понижая производительность компьютера. Учитывая рост появления новых вирусов, которые, однако, растут в геометрической прогрессии, это приведет к ситуации, когда антивирусная программа, использующая сигнатурный анализ, уже не сможет справиться с подобной борьбой из-за нехватки вычислительных ресурсов пользовательского компьютера. Поэтому «классический» подход к антивирусной защите, обнаружение вируса после появления его сигнатуры, становится уже менее эффективным в защите данных.

Ответом антивирусных компаний на такое положение дел, стало развитие антивирусов с принципами «облачных вычислений», т.е. антивирусы, не содержащие всей базы сигнатур вирусов на локальном ПК, а закачивающиеся по запросу в случае необходимости с удаленного сервера.

Согласно статистике сотрудника компании F-Secure Олега Федорова, вырисовывается такая картина: «Если сигнатура одного вируса занимает всего 20 байт, то 3 млн. вирусов - это почти 60 мегабайт (за один 2008 год - 15 миллионов). Всего спустя 5 лет это будет более гигабайта. И это ресурсы только для одного антивируса… Обычные пользователи ПК, не захотят тратить столько памяти для антивируса, проверять обновления каждый раз. Для ПК это нелегкая работа».[1]

Именно по этим причинам так быстро распространяется облачная технология.

Cloud-технологии – это облачные вычисления, представляющие собой технологию обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю в качестве интернет сервиса.[1] Идея, положенная в основу облачных антивирусных продуктов, достаточно проста. В ее основе лежит клиентская и серверная части cloud-антивируса. Первая имеет минимальный размер, устанавливается на машины пользователей и содержит в своем составе движок, сканирующий данные и отправляющий контрольные суммы файлов на сервер. Дислоцированный в облаках сервер принимает от клиентов хэши файлов, ищет их в базе сигнатур вирусов и выдает свой вердикт относительно чистоты присланных данных. В случае обнаружения зловредной программы, сервер отсылает клиенту соответствующие скрипты, выполнение которых очищает пользовательский компьютер от вредоносных объектов.

Подобная схема взаимодействия не только позволяет существенно снизить нагрузку на аппаратные ресурсы компьютера, но и освобождает от необходимости постоянно скачивать базы сигнатур, а также обеспечивает наилучшую защиту за счет применения системы "коллективного разума", использующей полученную от многомиллионной аудитории информацию для автоматического обнаружения и классификации новых видов вредоносных программ.

Как бы не казалось на первый взгляд отличным решением с огромными плюсами, но присутствует и обратная сторона медали/

Достоинства этих технологий в том, что:[3]

- Повышенная производительность;
- Очень быстрая защита в обнаружение нового вируса и добавлением его в базу;
- Поддержание актуальности базы данных угроз;
- Ускоренное внедрение новых средств борьбы с вредоносным ПО;
- Сведение к минимуму ложных срабатываний.

Недостатков тоже достаточно, но они возникают из-за использования облачных вычислений:[3]

- Проблемы загрузки сетевых подключений на медленных каналах связи;
- Постоянный доступ в интернет. Без соединения с «облаком» антивирусная система становиться неработоспособной и шанс обнаружения нового вируса у чисто “облачного” антивируса равен нулю;
- Конфиденциальность персональных данных не сохраняется в полную меру - отправленные данные будет доступно антивирусной компаний.
- В некоторых компаниях может быть запрещена отсылка файлов в Интернет.

Не смотря на то, что у облачной структуры плюсов больше, чем минусов, обычные антивирусные решения будут еще долго в спросе у пользователей, особенно в корпоративном секторе.

Кроме как чисто облачных антивирусов, присутствуют синтез «классического» и «облачного» антивируса. По поводу этого сочетания и взгляда на cloud computing, говорит Григорий Васильев, технический директор ESET:

«Применение in-the-cloud технологий призвано решить сразу несколько задач. Помимо уменьшения нагрузки на вычислительные мощности ПК, это глобальный мониторинг угроз и повышение оперативности работы разработчиков антивирусного ПО. Очевидно, что использование сигнатурных баз (а иногда и белых списков), размещенных не на компьютере пользователя, а на внешнем сервере, доступном через интернет-соединение, позволяет существенно сократить нагрузку на компьютер. Но при всех выгодах подобного подхода не стоит забывать и о присущих ему недостатках. «Облачный» антивирус может эффективно работать только при наличии доступа к Интернету, если точнее - к серверу вендора. Пожалуй, это самое узкое место «чистых» in-the-cloud систем, поскольку современным вредоносным программам не составляет труда заблокировать

доступ зараженного компьютера к определенным ресурсам сети. Например, широко известный червь Conficker блокировал доступ ПК пользователей к сайтам производителей антивирусов, к ресурсам обновлений Microsoft и пр. С нашей точки зрения, наиболее действенным является сочетание «облачных» технологий и полнофункциональной клиентской части антивируса, которая устанавливается на ПК пользователя. «Облачная» технология, использующаяся в продуктах ESET NOD32 с 2005 года, получила название ThreatSense.Net и представляет собой систему обратной связи с пользователями. Подозрительные файлы с согласия пользователя отсылаются в вирусную лабораторию, и в случае подтверждения вредоносности разработчики оперативно выпускают обновления, обеспечивающие защиту клиентов ESET во всём мире. Благодаря in-the-cloud составляющей разработчики антивирусного ПО могут анализировать активность вредоносного ПО, отслеживать эпидемии, развитие бот-сетей и своевременно реагировать на появление новых угроз. В то же время наличие полнофункциональной клиентской части позволяет обойти «узкое» место in-the-cloud технологий, поскольку за счет эвристических методов защита ПК обеспечивается даже в том случае, когда доступ к обновлениям продукта невозможен».[2]

В связи с постоянным наплывом новых вирусных и шпионских программных средств, с увеличением производительности для поиска вирусов «классическими» решениями, у технологий cloud computing довольно перспективное будущее. На сегодняшний день метод перевода части вычислительных процессов в «облака» становится более востребованным. Поэтому скоро перед большинством разработчиков встанет выбор: внедрять ли инновационные cloud computing технологии, либо сдаться «облачным» конкурентам и уйти со сцены антивирусных решений?

Библиографический список

1. Крупин А. Облачные антивирусы - в теории и на практике. Часть 1 / web: [Электронный ресурс]. Режим доступа: http://www.3dnews.ru/software/cloud-ativiruses-1/

2. Крупин А. "Облачный" антивирус / КОМПЬЮТЕРALAB – web: [Электронный ресурс]. Режим доступа: http://www.computerra.ru/terralab/ softerra/424961/

3. Сапоненко Д. Антивирусные системы с облачной архитектурой / web: [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/121197/

А.С. Королев, РГППУ
студент группы КТ-505
Руководитель: ст. преп. кафедры СИС
Е.В. Болгарина

ВНЕДРЕНИЕ SCORM В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС

В современном мире научно-техническая революция привела к быстро развивающимся процессам глобализации. В нашу жизнь вошло такое понятие, как «глобальное образование», которое выступает наиболее эффективным средством позитивного развития процессов глобализации, так как только образованное общество и образованное человечество может сохранить мир, избежать анархии и насилия, направив свои силы в сторону улучшения жизни, путем развития новейших технологий.

В XXI веке проблемы образования становятся приоритетными во всем мире, так как они определяют будущее каждой страны в отдельности и планеты в целом.[1]

Решить проблемы образования за короткий период времени будет достаточно сложно, потребуется разработка и принятие новых реформ, которые будут направлены на стандартизацию и глобализацию образования. Для перехода на новый этап перемен в образовании необходимо осуществить переход к