ПОСТРОЕНИЕ ЭФФЕКТИВНЫХ КОРПОРАТИВНЫХ СИСТЕМ АНТИВИРУСНОЙ ЗАЩИТЫ

А.М.Кобзарев[1] , З.М.Соловьёва[2]

[1] – студент 1 курса, факультета ЭУТ, группы ДКТ, Белорусского государственного экономического университета

[2] – научный руководитель, старший преподаватель кафедры информационных технологий, Белорусского государственного экономического университета, Минск, 220672, Партизанский пр., 26, тел.(8017) 249-19-81, e-mail: solovjeva@bseu.minsk.by.

Сегодня проблема построения эффективной корпоративной системы антивирусной защиты является одной из приоритетных при обеспечении безопасности корпоративных компьютерных сетей Internet/Intranet.

Актуальность данной проблемы объясняется следующими основными причинами:

лавинообразным ростом числа компьютерных вирусов. Так, например, в августе 1995года был обнаружен первый макровирус, а в настоящее время число известных макровирусов превысило отметку в 1000 штук и продолжает интенсивно расти. Данные последних независимых отчётов свидетельствуют о том, что средний уровень заражения вирусами корпоративных компьютерных сетей увеличился с 55% в 1995 году до 99,9% в 2001 году.

неудовлетворительным состоянием антивирусной защиты в существующих корпоративных компьютерных сетях. Сегодня сети российских и белорусских компаний находятся в постоянном развитии, соответственно растёт и число точек проникновения вирусов в корпоративные сети Internet/Intranet. Как правило , такими точками являются шлюзы и серверы Интернета, файл-приложений, групповой работы и электронной почты ; рабочие станции.

Проблемы корпоративного пользования

Обычная корпоративная компьютерная сеть включает в себя сотни рабочих станций, десятки серверов, активное и пассивное телекоммуникационное оборудование и , как правило имеет очень сложную структуру.

Стоимость обслуживания такой сети катастрофически растёт вместе с увеличением числа подключаемых рабочих станций. Сейчас многие решают проблему уменьшения совокупной стоимости владения или эксплуатации компьютерной инфраструктуры предприятия. Очевидно, расходы на антивирусную защиту являются не последним пунктом в списке общих расходов. Однако существует принципиальная возможность их снижения путём реализации централизованного управления антивирусной защитой корпоративной сети. Необходимо, чтобы администратор мог с единой консоли отслеживать все точки проникновения вирусов и эффективно управлять всеми присутствующими в сети предприятия антивирусными средствами как своего, так и стороннего производства. Цель такого управления – блокировать все возможные точки проникновения вирусов, а именно:

- проникновение вирусов на рабочие станции при использовании инфицированных файлов с переносных источников (флопи – диски, компакт – диски, Zip, Jazz, Floptical и т.д.);

- заражение вирусами с помощью бесплатного инфицированного программного обеспечения, полученного из Интернета и сохранённого на локальной рабочей станции;
- проникновение вирусов при подключении к корпоративной сети с помощью модема инфицированных рабочих станций удалённых и мобильных пользователей;
- заражение вирусами, инициированное удалённым сервером, подсоединённым к корпоративной сети и обменивающимся инфицированными данными с корпоративными серверами файл – приложений и баз данных;
- распространение электронной почты, содержащей в приложениях файлы Excel и Word , инфицироапнные макровирусами.

Сложность создания комплексного централизованного управления и стала камнем преткновения для успешного создания эффективных корпоративных систем антивирусной защиты, что в конечном счёте привело к столь широкому проникновению компьютерных вирусов в корпоративные сети Internet/Intranet.

Согласно отчётам компании Trend Micro, корпоративные пользователи постоянно сталкиваются с фактом проникновения вирусов в свои сети (см.табл.1).

Можно проверить свою рабочую станцию, и, в случае заражения компьютер- ными вирусами, вылечить её, воспользовавшись следующими инструкциями:

1) С заражённой машины зайти в бесплатную службу онлайнового сканирования HouseCall при помощи броузера (housecall.antivirus.com) .
2) Просканировать ПК . Выяснив имя вируса, зайти на сайт www.antivirus.com/vinfo и выполнить его поиск.
3) Прочитать описание вируса и выполнить инструкции по его удалению.

Приведём краткое описание некоторых вирусов, которые нанесли ущерб корпоративным сетям:

- **PE_FUNLOVE.4099** – это уже не новый резидентный вирус под Windows, который был недавно обнаружен несколькими интернет – пользователями. Данный вирус инфицирует файлы как на локальных, так и на сетевых дисках. При запуске инфицированного файла PE_FUNLOVE.4099 записывает файл **flcss.exe** в системный каталог Windows и пытается заразить все файла с расширениями .EXE, .OCX, .SCR. На системах Windows NT вирус PE_FUNLOVE.4099 пытается изменить **ntldr** и **ntoskrnl.exe** с целью дать всем пользователям права администратора. Это произойдёт после того, как пользователь с правами администратора зайдёт в систему и затем вы- полнит её перезагрузку;
- **TROJ_NAVIDAD.E** – это вариант TROJ_NAVIDAD.A , который был впервые обнаружен в ноябре 2000 года. Оригинальный TROJ_NAVIDAD.A содержит «ошибку» , которая приводит к тому, что при запуске .EXE – файла на экране пользователя появляется сообщение. В новом вирусе эта «ошибка» исправлена. Он корректно инсталлируется в системе после чего рассылает себя по всем адресам из адресной книги инфицированного пользователя в виде присоединённого файла **emanuel.exe**. Несмотря на то, что TROJ_NAVIDAD.E впервые был обнаружен в декабре 2000 года, он продолжает распространяться и по сей день;
- **PE_KRIZ.4050** – это старый 32-битный вирус под Windows, который был недавно обнаружен сразу во многих странах. Как и несколько других старых вирусов, PE_KRIZ.4050 смог вернуться, потому что был выпущен по ошибке в патче к компьютерной игре.

PE_KRIZ.4050 содержит деструктивную функцию, сходную с заложенной в PE_CIH,которая позволяет изменять данные в CMOS и обнулять BIOS;

- **VBS_FUNNY** – это новое семейство «червей» , написанных на Visual Basic Script, которые были недавно обнаружены в Европе. При запуске эти черви ищут определённый ключ в реестре и, если его нет, рассылают по почте сообщения с присоединённым вирусом по всем адресам из адресной книги Microsoft Outlook.

Если указанный ключ найден, то черви записывают на диск исполняемый файл startx.exe, который является известным «троянцем», похищающим пароли;

- **VBS_COLOMBIA** – это ещё один клон вируса VBS_LOVELETTER.A. несмотря на то, что оригинал получил мировое распространение, многочисленные его модификации не перестают появляться. VBS_COLOMBIA – это деструктивный вирус, который нацелен на файлы с расширениями: .VBS, .VBE, .JS, .JSE, .CSS, .WSH, .SCT, .HTA, .JPG, .JPEG, .MP3 и .MP2 .

Полное описание этих и других вирусов, а также механизмов их действия можно найти по адресу: www.antivirus.com/vinfo.

Эффективные решения антивирусной защиты корпоративной сети.

В настоящее время лидерами на рынке антивирусного ПО являются компании – производители Trend Micro, McAfee, Symantec и Computer Associates.Так, например, согласно отчёту International Data Corporation (IDC) компания Trend Micro является лидером по продажам антивирусной защиты для серверов и шлюзов Интернета с долей мирового рынка более 54%. Давайте рассмотрим предлагаемые ею решения более подробно.

Компания Trend Micro первой предложила концепцию антивирусного сканирования на уровне интернет-шлюза, представив свой продукт InterScan VirusWall в октябре 1995 года, и до сих пор продвигает инновационные решения на рынок антивирусных технологий.

Сегодня InterScan VirusWall является одним из наиболее стабильных антивирусных решений защиты и фильтрации информации интернет – шлюзов для наиболее распространённых платформ семейства UNIX и Windows – например, Red Hat Linux, SuSE Linux и Turbo Linux, а также Windows NT, Solaris и HP-UX. С помощью сканирования и обнаружения вирусов и враждебных программ в траффиках HTTP, SMTP, и FTP VirusWall помогает останавливать их до того, как они достигнут рабочих станций.

Принцип действия InterSkan VirusWall заключается в следующем: он обеспечивает сканирование «три-в-одном» в режиме реального времени на уровне интернет – шлюза для защиты от вирусов и враждебных программ. InterSkan применяет технологии распознавания, основанные на использовании соответствующих правил и сигнатур.

Антивирусная защита независимо от платформы может управляться как составная часть корпоративной антивирусной защиты.

Другим интересным решением Trend Micro является интегрированное семейство антивирусных продуктов для среды Lotus Notes под названием Trend Enterprise Solution Suite (TESS) for Lotus Notes. Оно представляет собой комплексную антивирусную защиту рабочих станций, файловых серверов, интернет – шлюза и возможность централизованного управления антивирусной защитой для предприятий, использующей Lotus Notes для обмена сообщениями и групповой работы.

Примечательно, что окружение Notes остается популярным среди крупных компаний и организаций, которым необходима высокомасштабируемая и надежная платформа для обеспечения совместной работы. Так, например, консалтинговая и маркетинговая фирма «Radicati Group» оценивает количество крупнейших компаний , которые выбрали Lotus Notes в качестве корпоративного стандарта системы обмена сообщениями,в 29 %.

Trend Enterprise Solution Suite (TESS) for Lotus Notes объединяет в одном комплексе следующие антивирусные средства :

- **InterScan VirusWall** сканирует все трафики HTTP, SMTP, и FTP на уровне интернет – шлюза , обеспечивая фильтрацию почтовых сообщений, загружаемых файлов и доступ к web-сайтам , на наличие разрушительных Java – апплетов и управляющих элементов ActiveX;
- **ServerProtect** защищает многочис – ленные файл – серверы Windows NT и Novell Netware, а уведомления и протоколирование помогают администраторам отслеживать все случаи вирусного заражения;
- **OfficeScan Corporate Edition** сочетает онлайновую защиту рабочих станций с лёгкостью серверного управления;
- **ScanMail for Lotus Notes** обнаруживает и удаляет вирусы из почты Notes , совместно используемых баз данных , а также в процессе репликации;
- **Trend Virus Control System (Trend VCS)** предоставляет управление всеми этими продуктами с помощью единой web- или windows-консоли.

Существенно, что один из первых продуктов для Notes, сертифицированный ICSA (Международной ассоциацией компьютерной безопасности) как продукт, обнаруживающий 100% вирусов из списка in-the-wild, ScanMail for Lotus Notes остаётся единственным антивирусным решением, поддерживающим полный спектр корпоративных вычислительных платформ для Notes, включая Windows NT/2000 , Solaris , IBM eServer pSeries (бывший AIX) .

Заключение

По мнению аналитиков IDC, рынок продаж антивирусного ПО вырастет с 1,2 млрд. долларов в 1999/2000 году до 2,7 млрд. долларов в 2004 году с планируемым темпом роста 17%. При этом преобладающие значение приобретают решения антивирусной защиты серверов и интернет-шлюзов, интегрированные с другими решениями в области безопасности копьютерных сетей, например с IDS (системами обнаружения вторжений) и с др.

Все вместе это лишний раз подчеркивает, что проблема построения эффективной корпоративной системы антивирусной защиты Internet/Intranet назрела и требует незамедлительного решения в российских и белорусских компаниях.

Литература

1.Петренко С. «Безопасность на высшем уровне», журнал CHIP, май 2001г.

2.Различне положения и данные из различных номеров «Компьютерной газеты»

3.Использование ресурсов Internet.

№	10 наиболее распространённых вирусов in-the-wild	10 вирусов, которые наиболее часто появляются в корпоративных сетях	10 наиболее распространённых вирусов на начало 2001года.
1	TROJ_MTX.A	VBS_ KAKWORM.A	VBS_ KAKWORM.A
2	TROJ_HYBRIS.B	TROJ_MTX.A	TROJ_PRETTY_PARK
3	VBS_KAKWORM.A	JOKE_WOW	TROJ_SKA
4	TROJ_HYBRIS.A	W97M_ASSILEM.B (Melissa)	VBS_LOVELETTER
5	TROJ_BYMER	TROJ_HYBRIS.B	PE_CIH
6	TROJ_NAVIDAD.E	JOKE_BURPER	W97M_MELISSA
7	TROJ_PRETTY_PARK	TROJ_BYMER	TROJ_MTX.A
8	TROJ_CLICK	VBS_LOVELETTER	TROJ_QAZ.A
9	TROJ_HYBRIS.D	W97M_THUS	W97M_ETHAN.A
10	TROJ_SUB7.BONUS	TROJ_PRETTY_PARK	O97M_TRISTATE

Таблица 1. Вирусы, которые наиболее часто появляются в корпоративных сетях.