Системное администрирование компьютерной сети. Надежность и безопасность.

Копытов М.А., Рогов Ю.П.
Вычислительный центр РАН, Москва

Одной из главных задач системного администратора является обеспечение надежности и безопасности компьютерной сети.

Задачи обеспечения надежности и безопасности близки по своему содержанию, но имеется ряд принципиальных отличий, существенным образом влияющих на методику решения этих задач.

Задача обеспечения надежности связана с изучением слабых мест в системе, выявлением ошибок в системных программах, с заменой одних элементов системы на другие, более надежные, а также с совершенствованием программно-аппаратных средств, определяющих работу системы.

Обеспечение надежности предполагает также организацию такой методики использования программно-аппаратных средств, при которой возможные отказы системы не приводили бы к длительным простоям и потере пользовательской и системной информации.

Обеспечение безопасности системы в первую очередь зависит от так называемого человеческого фактора, поскольку защищаться приходится от тех, кто случайным образом или умышленно становится пользователем системы, не имея на то законного права. Цели проникновения в систему могут быть следующими:

- компьютерное хулиганство;
- незаконное использование ресурсов системы;
- поиск и незаконное чтение чужой информации;
- порча информации или ее подмена;
- вывод из строя системы.

Семилетний опыт использования ЛВС ВЦ РАН позволил нам накопить некоторый опыт борьбы с компьютерными нарушителями и разного рода хакерами.

Исходя из того, что вывод из строя системы для взломщика является крайне редкой целью, и чаще всего несанкционированный доступ производится с целью использования системы для проникновения в другие сети или порою из тщеславия, стремления самоутвердиться таким своеобразным способом, мы и строим свою политику при борьбе с этими преступниками. Тем более, что российское законодательство с некоторых пор предусматривает наказание и за этот вид правонарушений.

Как известно, любую систему, у которой есть внешняя коннективность, можно взломать - ограничено это только сроками и использованием для этого вычислительных мощностей. Поэтому меры повышения безопасности нами принимаются по мере накапливания опыта в борьбе с нарушителями, по рекомендациям международных и отечественных организаций, занимающихся этими проблемами.

При надежно функционирующей локальной сети главным объектом заботы администратора должны быть пользователи сети. То есть, при обеспечении необходимой безопасности работы всей системы и защиты ее от несанкционированного доступа, не стоит делать это за счет уменьшения возможностей своих же пользователей и снижения эффективности их работы.

Подробно излагать меры по повышению уровня надежности и безопасности системы - дело неблагодарное. Статьи, подобные этой, не

должны быть руководством для хакеров. Поэтому ограничимся перечислением лишь некоторых мероприятий, связанных с данной проблемой:

– все наше IP-адресное пространство разделено на внутреннее и внешнее;
– внутренние IP-адреса недоступны как извне, так и с внешних адресов (за исключением особых случаев);
– повышена защита web-сервера и почтового сервера (антирелэй);
– регулярно проводится реконфигурация внешнего маршрутизатора (фильтрация портов);
– произведено разделение серверов по функциям: web-сервер, почтовый сервер, файловый сервер, NIS-сервер и др.

В заключение еще несколько общих соображений по методике администрирования.

Наличие квалифицированных и постоянных административных служб - очень важный фактор в деле повышения надежности и безопасности компьютерной сети.

В нашем институте административные сетевые службы придерживаются следующего принципа работы: для того чтобы системный администратор лучше чувствовал проблемы рядового пользователя и быстрее реагировал на различные системные зависания, сбои и замедление реакции на выполнение своих задач, он не должен сам работать на самом мощном сервере, особом индивидуальном дисковом устройстве и в отдельном адресном (IP-addresses) пространстве. Его среда должна быть обычной пользовательской средой.

Сколько должно быть администраторов? В идеале - один, хотя это чревато огромной зависимостью от фигуры этого специалиста. При этом могут возникать большие проблемы при его длительном отсутствии и уж совсем плохо, если по каким-либо причинам он прекращает выполнять свои функции. Поэтому нужно искать золотую середину. Например, один главный администратор, отвечающий за работу всей сети и один-два человека, отвечающие за какой-либо отдельный компонент сети, а также способные в какой-то части подстраховать главного. В любом случае этот узкий круг специалистов должен быть коллективом единомышленников, абсолютно доверяющих друг другу и соответствующим материальным и моральным образом поддерживаться администрацией своего института.

ЛИТЕРАТУРА

1. Байкова И.В., Копытов М.А., Кулагин М.В., Метелкин А.В., Михайлов Г.М., Плечов П.Ю., Рогов Ю.П. Распределенные информационно-вычислительные системы. Выпуск 2. Инфраструктура и базовые средства локальной сети ВЦ РАН, М.: Вычислительный центр РАН, 1996. - 96с.
2. Михайлов Г.М., Копытов М.А., Кулагин М.В., Рогов Ю.П. Информационно-вычислительная система ВЦ РАН Сб. "Развитие информационно-вычислительной системы ВЦ РАН", ВЦ РАН, М., 1998, С.7-22
3. Копытов М.А., Рогов Ю.П. Системное администрирование компьютерной сети Сб. "Развитие информационно-вычислительной системы ВЦ РАН", ВЦ РАН, М., 1998, С.38-47