### **Классификация угроз**

Универсальной классификации угроз не существует, возможно, и потому, что нет предела творческим способностям человека, и каждый день применяются новые способы незаконного проникновения в сеть, разрабатываются новые средства мо­ниторинга сетевого графика, появляются новые вирусы, находятся новые изъяны в существующих программных и аппаратных сетевых продуктах. В ответ на это разрабатываются все более изощренные средства защиты, которые ставят пре­граду на пути многих типов угроз, но затем сами становятся новыми объектами -атак. Тем не менее попытаемся сделать некоторые обобщения. Так, прежде всего угрозы могут быть разделены на **умышленные и неумышленные.**

***Неумышленные угрозы*** вызываются ошибочными действиями лояльных сотруд­ников, становятся следствием их низкой квалификации или безответственности. Кроме того, к такому роду угроз относятся последствия ненадежной работы про­граммных и аппаратных средств системы. Так, например, из-за отказа диска, кон­троллера диска или всего файлового сервера могут оказаться недоступными данные, критически важные для работы предприятия. Поэтому вопросы безопас­ности так тесно переплетаются с вопросами надежности, отказоустойчивости тех­нических средств. Угрозы безопасности, которые вытекают из ненадежности работы программно-аппаратных средств, предотвращаются путем их совершен­ствования, использования резервирования на уровне аппаратуры (RAID-масси­вы, многопроцессорные компьютеры, источники бесперебойного питания, кла­стерные архитектуры) или на уровне массивов данных (тиражирование файлов, резервное копирование).

***Умышленные угрозы*** могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например, нарушение целостности и доступности информации, приведение в нерабочее со­стояние приложений и устройств. Так, умышленные угрозы возникают в резуль­тате деятельности хакеров и явно направлены на нанесение ущерба предпри­ятию.

В вычислительных сетях можно выделить следующие типы умышленных угроз:

* незаконное проникновение в один из компьютеров сети под видом легально­го пользователя;
* разрушение системы с помощью программ-вирусов;
* нелегальные действия легального пользователя;
* «подслушивание» внутрисетевого графика.

***Незаконное проникновение*** может быть реализовано через уязвимые места в сис­теме безопасности с использованием недокументированных возможностей опе­рационной системы. Эти возможности могут позволить злоумышленнику «обой­ти» стандартную процедуру, контролирующую вход в сеть.

Другим способом незаконного проникновения в сеть является использование «чу­жих» паролей, полученных путем подглядывания, расшифровки файла паролей, подбора паролей или получения пароля путем анализа сетевого графика. Осо­бенно опасно проникновение злоумышленника под именем пользователя, наде­ленного большими полномочиями, например администратора сети. Для того чтобы завладеть паролем администратора, злоумышленник может попытаться войти в сеть под именем простого пользователя. Поэтому очень важно, чтобы все пользо­ватели сети сохраняли свои пароли в тайне, а также выбирали их так, чтобы мак­симально затруднить угадывание.

Подбор паролей злоумышленник выполняет с использованием специальных про­грамм, которые работают путем перебора слов из некоторого файла, содержаще­го большое количество слов. Содержимое файла-словаря формируется с учетом психологических особенностей человека, которые выражаются в том, что чело­век выбирает в качестве пароля легко запоминаемые слова или буквенные соче­тания.

Еще один способ получения пароля — это внедрение в чужой компьютер «троян­ского коня». Так называют резидентную программу, работающую без ведома хозяи­на данного компьютера и выполняющую действия, заданные злоумышленником. В частности, такого рода программа может считывать коды пароля, вводимого пользователем во время логического входа в систему.

Программа-«троянский конь» всегда маскируется под какую-нибудь полезную ути­литу или игру, а производит действия, разрушающие систему. По такому прин­ципу действуют и ***программы-вирусы****,* отличительной особенностью которых яв­ляется способность «заражать» другие файлы, внедряя в них свои собственные копии. Чаще всего вирусы поражают исполняемые файлы. Когда такой испол­няемый код загружается в оперативную память для выполнения, вместе с ним получает возможность исполнить свои вредительские действия вирус. Вирусы могут привести к повреждению или даже полной утрате информации.

***Нелегальные действия легального пользователя*** *—* этот тип угроз исходит от ле­гальных пользователей сети, которые, используя свои полномочия, пытаются вы­полнять действия, выходящие за рамки их должностных обязанностей. Напри­мер, администратор сети имеет практически неограниченные права на доступ**ко**всем сетевым ресурсам. Однако на предприятии может быть информация, до­ступ к которой администратору сети запрещен. Для реализации этих ограниче­ний могут быть предприняты специальные меры, такие, например, как шифрова­ние данных, но и в этом случае администратор может попытаться получить дос­туп к ключу. Нелегальные действия может попытаться предпринять и обычный пользователь сети. Существующая статистика говорит о том, что едва ли не по­ловина всех попыток нарушения безопасности системы исходит от сотрудников предприятия, которые как раз и являются легальными пользователями сети.

***«Подслушиванием внутрисетевого трафика*** *—* это незаконный мониторинг сети, захват и анализ сетевых сообщений. Существует много доступных программных и аппаратных анализаторов трафика, которые делают эту задачу достаточно три­виальной. Еще более усложняется защита от этого типа угроз в сетях с глобаль­ными связями. Глобальные связи, простирающиеся на десятки и тысячи кило­метров, по своей природе являются менее защищенными, чем локальные связи (больше возможностей для прослушивания трафика, более удобная для злоумыш­ленника позиция при проведении процедур аутентификации). Такая опасность одинаково присуща всем видам территориальных каналов связи и никак не зави­сит от того, используются собственные, арендуемые каналы или услуги общедос­тупных территориальных сетей, подобных Интернету.

Однако использование общественных сетей (речь в основном идет об Интерне­те) еще более усугубляет ситуацию. Действительно, использование Интернета добавляет к опасности перехвата данных, передаваемых по линиям связи, опас­ность несанкционированного входа в узлы сети, поскольку наличие огромного числа хакеров в Интернете увеличивает вероятность попыток незаконного про­никновения в компьютер. Это представляет постоянную угрозу для сетей, под­соединенных к Интернету.

Интернет сам является целью для разного рода злоумышленников. Поскольку Интернет создавался как открытая система, предназначенная для свободного об­мена информацией, совсем не удивительно, что практически все протоколы стека TCP/IP имеют «врожденные» недостатки защиты. Используя эти недостатки, злоумышленники все чаще предпринимают попытки несанкционирован­ного доступа к информации, хранящейся на узлах Интернета.