УДК 004.71

И.И. Прокопов

Структурирование угроз в корпоративной сети

Рассматриваются некоторые виды угроз в локальной сети. Предполагается, что в сети имеются авторизованные рабочие станции, посредством которых осуществляется доступ к конфиденциальной информации организации, в том числе к персональным данным. В сети могут находиться также рабочие станции, которые не подчиняются общей политике безопасности.

Ключевые слова: угроза, локальная сеть, информационная безопасность, интернет.

Рассмотрим классификацию угроз применительно к случаю локальной сети, которая используется как для общей организации работы, так и для доступа к конфиденциальной информации предприятия. Предполагается обработка персональных данных без использования Интернет-соединений, т.е. локальная сетевая обработка в организации типа учебного заведения (институт, университет). Можно рассматривать такую локальную сеть как открытую распределенную среду, в которой пользователи со своих рабочих станций должны иметь возможность доступа к услугам на серверах в сети [1]. В большинстве случаев в этой же сети имеются рабочие станции, которые не осуществляют обработку конфиденциальной информации, но имеют выход в Интернет, связь с другими ЭВМ в локальной сети, в том числе с серверами, хранящими персональные данные.

Угрозы, связанные с особенностями функционирования рабочих станций сети

Некоторые виды угроз связаны со слабой контролируемостью рабочих станций (подмена пользователя, подмена рабочей станции, перехват сообщений в среде передачи) [1].

Модель телекоммуникационной системы доступа к данным имеет следующие основные особенности:

– масштабируемость по количеству точек доступа к данным (сотни и тысячи);

– удаленность и автономность пользователей клиентских компьютеров;

– неподконтрольность пользователей нижнего уровня политикам безопасности (самоадминистрирование).

Данные особенности могут привести к реализации следующих угроз:

– заражение вирусами соседних компьютеров в сети;

– кража секретного ключа для доступа к данным с авторизованной рабочей станции;

– негативное воздействие на другие рабочие станции сети (сетевые атаки).

Угрозы, связанные с Интернет-подключениями рабочих станций

При наличии такого подключения возможна организация виртуального канала связи, при котором на ПЭВМ организуется сервер по передаче данных в Интернет. К такому типу соединений относятся популярные сейчас P2P-соединения. ЭВМ-участники такого проекта становятся узлами распределенной сети, являющейся подмножеством Интернет. При этом в случае внедрения зараженного ПО на рабочую станцию она может стать источником информации, в том числе конфиденциальной, а также источником инсайдерских атак, управляемых из Интернет, и источником вирусов в сети. Например, по сведениям разработчиков антивирусного ПО, такого рода соединения привели к распространению новой волны вируса Conficker в начале апреля 2009 г.

При наличии Интернет-подключения рабочей станции в локальной сети угрозы можно разделить на две группы:

– связанные с инсайдерскими атаками посредством управляемой из Интернет рабочей станции;

– возможность для корпоративного пользователя осуществлять внешнюю атаку на периметр своей сети посредством управляемого им внешнего хоста.

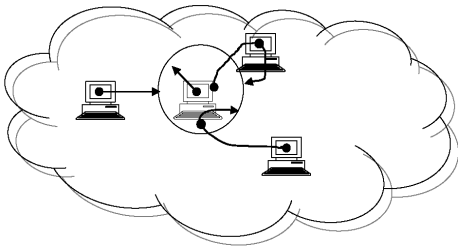

Рис. 1. Угрозы при наличии Интернет-подключения

Также при этом могут быть реализованы угрозы чисто внешние и внутренние. Схематично 4 вида угроз изображены на рис. 1.

Угрозы, связанные с организацией несанкционированных подключений

В настоящее время актуальной задачей является настройка политики незашифрованных данных в сетях (в связи с безопасностью). С точки зрения соблюдения политик безопасности в целом всю сеть можно разделить на две части: хорошо контролируемые зоны

и плохо контролируемые зоны. К хорошо контролируемым зонам отнесем подразделения или их части, в которых работают обычные пользователи, настройки политик для их рабочих станций, принудительно внедренные и неизменяемые пользователем, и контролируемые администратором сети. К такому типу можно отнести практически все подразделения административного аппарата. Ко второму типу можно отнести подразделения нижнего уровня иерархии, например кафедры, лаборатории и т.п. При наличии в сети плохо контролируемых рабочих станций становится возможной организация нелегальной точки доступа в данную сеть для других «чужих» ПК.

Рынок достаточно дешевых сетевых устройств позволяет организовать несанкционированные подключения по современным технологиям – проводным и беспроводным:

• на базе точек доступа Wi-Fi, которые в современных моделях ПК могут быть встроенными;

• на базе терминалов сотовой связи;

• на базе адаптеров Wire-Wireless для LAN, USB и т.п. при наличии физического доступа к портам сетевых устройств и ПК;

• на базе обычной телефонной связи общего пользования с использованием обычных и ADSL модемов;

• на базе устройств для организации связи через инфраструктурные силовые (электрические) и информационные (радиовещание) сети.

Подобные устройства и адаптеры позволяют несанкционированно подключить к корпоративной сети другие сети разного размера, в том числе и весь Интернет. При этом средства защиты сети, рассчитанные на атаки со стороны внешнего периметра, работать не будут.

В качестве защитных мер следует применять изоляцию сегментов сети и отдельных узлов друг от друга [2, 3]. Если требуется, обмен осуществляется через сервер с контролем содержимого посредством межсетевого экрана.

В ряде случаев можно снизить вероятность реализации угроз pt в отношении сервера. Введем в качестве одного из параметров обеспечения безопасности время t. Для устранения угроз в отношении сервера со стороны локальной сети можно использовать отключение сервера от сети с помощью аппаратного файрвола. Промежуток времени, в течение которого производится отключение, – это нерабочие часы из интервала [ts, te], задаваемые по расписанию ежедневно, а также в выходные и праздничные дни. Также сюда требуется включить временные интервалы, во время которых производятся профилактические работы и перенастройки на сервере. При этом можно считать, что на интервале [ts, te] величина pt будет равна нулю.

В корпоративной сети можно выделить следующие виды угроз:

– угрозы, связанные с особенностями функционирования рабочих станций сети;

– угрозы, связанные с наличием Интернет-подключений к части рабочих станций;

– угрозы, связанные с организацией несанкционированных подключений и с использованием одной общей среды передачи.

При использовании управляемых интеллектуальных устройств можно уменьшить вероятность реализации угроз как в отношении рабочих станций, так и в отношении серверов.

Литература

1. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд.: пер. с англ. – М.: Изд. дом «Вильямс», 2001. – 672 с.

2. Уэнстром М. Организация защиты сетей Cisco.: пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 768 с.

3. Хилл Б. Полный справочник по Cisco.: пер. с англ. – М.: Изд. дом «Вильямс», 2008. – 1088 с.

Прокопов Игорь Игоревич
ГОУ ВПО «Южно-Уральский государственный университет»,
доцент каф. цифровых радиотехнических систем
Эл. адрес: sub@drts.susu.ac.ru

I.I. Prokopov

Structurization of threats of a corporate network

Some kinds of threats in a local network are considered. It is supposed,that in a network there are authorized workstations by means of which access is provided to the confidential information of the organization,including to personal data. In a network there can be also workstations which do not submit to the general policy of safety.

Keywords: threat, local network,information security, Internet.