УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ БИЗНЕС-СИСТЕМ

Н.Н. Поснов, В.П. Киреенко
УО «Государственный институт управления и социальных технологий БГУ»,
г. Минск, Республика Беларусь

Усилия, направленные на защиту корпоративной информации, пока значительно отстают от темпов разработки стратегий развития электронного бизнеса. Между тем, проблемы безопасности обостряются с каждым днем, особенно в связи со стремительным развитием интернет-торговли и широким распространением сетей интранет/экстранет.

По мере возрастания роли, которую компьютеры и сетевые ресурсы начинают играть в ключевых процессах электронного и мобильного бизнеса, они становятся все более уязвимыми по отношению к внешним сетевым атакам. Как известно, средства электронного бизнеса предоставляют клиентам, партнерам и поставщикам доступ к корпоративным сетям и ресурсам, т. е. к тем самым информационным активам компаний, которые в традиционной бизнес-среде находятся на замке.

В современных условиях проблемы сохранения этих активов нарастают, как снежный ком, и способность обеспечить требуемый уровень защиты корпоративных ресурсов уже превратилась в фактор выживания компаний в конкурентной борьбе.

Заметим, что в общем случае под угрозой принято понимать потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. В свою очередь, угроза информационной безопасности автоматизированной системы – это возможность реализации воздействия на информацию,

обрабатываемую в информационной системе (ИС), приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты ИС, приводящего к их утрате, уничтожению или сбою функционирования [1, с. 28].

Классификация угроз может быть проведена по множеству признаков. Наиболее распространенными из них являются следующие.

1. По природе возникновения принято выделять естественные и искусственные угрозы.

Естественными принято называть угрозы, возникшие в результате воздействия на ИС объективных физических процессов или стихийных природных явлений, не зависящих от человека. В свою очередь, искусственные угрозы вызваны действием человеческого фактора.

Примерами естественных угроз могут служить пожары, наводнения, цунами, землетрясения и т. д. Неприятная особенность таких угроз – чрезвычайная трудность или даже невозможность их прогнозирования [1, с. 32].

2. По степени преднамеренности выделяют случайные и преднамеренные угрозы.

Случайные угрозы бывают обусловлены халатностью или непреднамеренными ошибками персонала. Преднамеренные угрозы обычно возникают в результате направленной деятельности злоумышленника.

В качестве примеров случайных угроз можно привести непреднамеренный ввод ошибочных данных, неумышленную порчу оборудования. Пример преднамеренной угрозы – проникновение злоумышленника на охраняемую территорию с нарушением установленных правил физического доступа [1, с. 41].

3. В зависимости от источника угрозы принято выделять:

Угрозы, источником которых является природная среда. Примеры таких угроз – пожары, наводнения и другие стихийные бедствия.

Угрозы, источником которых является человек. Примером такой угрозы может служить внедрение агентов в ряды персонала ИС со стороны конкурирующей организации.

Угрозы, источником которых являются санкционированные программно-аппаратные средства. Пример такой угрозы – некомпетентное использование системных утилит.

Угрозы, источником которых являются несанкционированные программно-аппаратные средства. К таким угрозам можно отнести, например, внедрение в систему «троянских коней» [2, с. 21–25].

4. По положению источника угрозы выделяют:

• Угрозы, источник которых расположен вне контролируемой зоны. Примеры таких угроз:

– перехват побочных электромагнитных излучений (ПЭМИН) или перехват данных, передаваемых по каналам связи;

– дистанционная фото- и видеосъемка;

– перехват акустической информации с использованием направленных микрофонов.

• Угрозы, источник которых расположен в пределах контролируемой зоны.

Примерами подобных угроз могут служить применение подслушивающих устройств или хищение носителей, содержащих конфиденциальную информацию [2, с. 26–27].

5. По степени воздействия на ИС выделяют пассивные и активные угрозы. Пассивные угрозы при реализации не осуществляют никаких изменений в составе и структуре ИС.

Реализация активных угроз, напротив, нарушает структуру информационной системы.

Примером пассивной угрозы может служить несанкционированное копирование файлов с данными [2, с. 35–37].

6. По способу доступа к ресурсам ИС выделяют:

– Угрозы, использующие стандартный доступ. Пример такой угрозы – несанкционированное получение пароля путем подкупа, шантажа, угроз или физического насилия по отношению к законному обладателю.

– Угрозы, использующие нестандартный путь доступа. Пример такой угрозы – использование недекларированных возможностей средств защиты [2, с. 46–48].

Критерии классификации угроз можно продолжать, однако на практике чаще всего используется следующая основная классификация угроз, основывающаяся на трех введенных ранее базовых свойствах защищаемой информации:

1. Угрозы нарушения конфиденциальности информации, в результате реализации которых информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.

2. Угрозы нарушения целостности информации, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием ИС.

3. Угрозы нарушения доступности информации, возникающие в тех случаях, когда доступ к некоторому ресурсу ИС для легальных пользователей блокируется.

Необходимо отметить, что реальные угрозы информационной безопасности далеко не всегда можно строго отнести к какой-то одной из перечисленных категорий. Так, например, угроза хищения носителей информации может быть при определенных условиях отнесена ко всем трем категориям.

Перечисление угроз, характерных для той или иной информационной системы, является важным этапом анализа уязвимостей ИС, проводимого, например, в рамках аудита информационной безопасности, и создает базу для последующего проведения анализа рисков. Выделяют два основных метода перечисления угроз:

1. Построение произвольных списков угроз. Возможные угрозы выявляются экспертным путем и фиксируются случайным и неструктурированным образом.

Для данного подхода характерны неполнота и противоречивость получаемых результатов.

2. Построение деревьев угроз. Угрозы описываются в виде одного или нескольких деревьев. Детализация угроз осуществляется сверху вниз, и в конечном итоге каждый лист дерева дает описание конкретной угрозы. Между поддеревьями в случае необходимости могут быть организованы логические связи [3, с. 71–72].

Ниже кратко охарактеризованы наиболее распространенные типы сетевых угроз.

Вирусы

Эта наиболее часто встречающаяся форма нарушения системы безопасности. Вирус представляет собой программу или фрагмент программного кода, который незаметно загружается на компьютеры организации из сети и затем функционирует на них вопреки воле пользователей. Вирусы способны сами присоединяться к другим программам или файлам. Большинство вирусов обладают способностью к саморепликации и быстро заполняют имеющуюся память компьютера. Многие вирусы обеспечивают собственное распространение по вычислительным сетям [4].

Анализатор пакетов

Анализатор пакетов представляет собой приложение, использующее сетевой адаптер для захвата всех пакетов, транспортируемых через сеть. В настоящее время подобное программное обеспечение (ПО) широко используется в сетях на законных основаниях, прежде всего в целях анализа трафика, устранения выявленных неисправностей и профилактики потенциальных сбоев. Вместе с тем, поскольку некоторые сетевые приложения (в частности, работающие по протоколам HTTP, FTP, IMAP, SMTP, POP3) отсылают данные в простом текстовом формате, анализатор пакетов может применяться для получения конфиденциальной информации, например, регистрационных имен и паролей пользователей [4].

Имитация IP-адреса

При сетевой атаке этого типа хакер пытается выдать себя за лицо, наделенное широкими полномочиями, скажем, правами администратора. Подобная имитация осуществляется одним из двух способов: хакер может использовать либо IP-адрес из диапазона «доверенных» IP-адресов данной сети, либо авторизованный внешний IP-адрес, который также является «доверенным», и доступ с которого разрешен к определенным сетевым ресурсам. Имитация IP-адреса частенько предваряет атаки других типов. Классическим примером может служить атака, приводящая к отказам в обслуживании, при которой для собственной маскировки хакеры используют сымитированные IP-адреса источника.

Атаки с применением паролей

Атаки данного типа также предполагают использование различных схем, включая метод «грубой силы», троянских коней, имитацию IP-адресов или захват пакетов. Несмотря на то, что последние два метода позволяют выяснить регистрационные имена и пароли пользователей, атаки с применением паролей чаще всего базируются на повторяющихся попытках узнать сетевые идентификаторы пользователя. Этот способ как раз и называется методом «грубой силы». Его практическая реализация базируется на специально написанной программе, которая запускается в сетевой среде и пытается зарегистрироваться на сетевом ресурсе с разделяемым доступом, например, на сервере.

После того как эти попытки увенчаются успехом, хакер получит такие же права, как и пользователь с соответствующим именем и паролем. В том случае, когда права этого пользователя достаточно широки, хакер получает возможность создать для себя «черный ход», через который впоследствии он сможет получать доступ к желаемому ресурсу, причем независимо от последующих изменений пользовательских паролей.

Атака типа «отказ в обслуживании» DDOS

На этот раз хакер получает доступ к нескольким компьютерам, подключенным к Интернету, и инсталлирует на них специальное программное обеспечение. Затем по определенному сигналу все эти компьютеры начинают одновременно посылать данные на атакуемые web-сайты. Как правило, неожиданный всплеск сетевого трафика не может быть корректно обработан сервером и сетевым сегментом, к которому тот подключен. В результате производительность сервера резко падает, и в конечном счете сайт становится неработоспособным.

Вторжение в передачу данных

Чтобы вторгнуться непосредственно в процесс передачи данных, хакер должен получить доступ к пакетам, транспортируемым по сети. В роли хакера здесь может выступить сотрудник компании-провайдера, имеющий доступ ко всем пакетам, передаваемым между сетью провайдера и какой-либо другой сетью. Подобные атаки нередко требуют применения анализаторов сетевых пакетов, а также анализаторов протоколов сетевого и транспортного уровней.

Целями, которые хакер преследует в данном случае, могут быть кража конфиденциальной информации, вторжение в установленный сетевой сеанс для получения доступа к ресурсам частной сети, анализ трафика для извлечения сведений о сети и ее пользователях, инициация отказа в обслуживании, повреждение передаваемых данных либо умышленное добавление информации в передаваемый трафик.

Физическое нарушение функционирования

На сей раз злоумышленники получают доступ к центру обработки данных или выкрадывают оборудование. Для предотвращения атак данного типа администратор службы безопасности не должен ограничивать свою деятельность запиранием служебных помещений на ключ. Нередки ситуации, когда центры обработки данных являются наиболее ценным из всех корпоративных активов. Кража портативных компьютеров остается весьма распространенным явлением, сопряженным с большими финансовыми потерями, причем не столько из-за стоимости аппаратных средств, которые придется покупать взамен исчезнувших, сколько в связи с ценностью хранившейся на них конфиденциальной информации.

ЛИТЕРАТУРА

1. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин – М.: Академический Проект – 2005. – 268 с.

2. Ховард, М. 24 смертных греха компьютерной безопасности / М. Ховард, Д. Виега, Д. Лебланк, Д. Вьега – СПб.: Питер – 2010. 612 с.

3. Молдовян, А.А. Безопасность глобальных сетевых технологий / А.А. Молдовян, В. Зима, Н.А. Молдовян – СПб.: БХВ-Петербург. – 2002. – 422 с.

4. Поснов, Н.Н. Угрозы и точки уязвимости информационных систем // Н.Н. Поснов. Обеспечение общественной безопастности в Республике Беларусь: научные и прикладные аспекты. Тез. Докл. XIII Межвузовской научно-практической конференции, Минск 12 мая 2011 г. / Военная академия Республики Беларусь; редкол.: О.В. Шелков [и др.]. – Минск: Издательство УО «Военная академия Республики Беларусь». – С. 54–56.