Г. С. Курганская
(д.ф.-м.н., заведующая кафедрой информационных технологий в управлении)
Байкальская международная бизнес-школа
Иркутского государственного университета

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПАНИИ

Информационные технологии являются одним из ключевых факторов, обеспечивающим деятельность любой компании на всех управления, при этом масштаб компании только повышает их роль. Поэтому для эффективной работы компании существенным, а часто и жизненно необходимым, является надежное, бесперебойное функционирование всего комплекса информационных систем. Это безусловное требование приводит к необходимости поддержания постоянного, достаточно высокого уровня информационной безопасности.

Информационная безопасность организации — целенаправленная деятельность ее органов и должностных лиц с использованием разрешенных сил и средств по достижению состояния защищённости информационной среды организации, обеспечивающее её нормальное функционирование и динамичное развитие.

Следовательно, защита информации представляет собой комплекс мер, принятых для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним.

Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологи. С одной стороны стремительно развиваются средства работы с информацией в компаниях, для которых не подходят уже имающиеся системы защиты информации. Например, беспроводные локальные сети WiFi имеют ряд специфических уязвимостей, и для их защиты нужны новые средства. И, конечно, постоянно прогрессируют методы взлома информационных систем. Поэтому нужно четко понимать, что защита информации есть непрерывный процесс, и нет такого программного продукта, который бы обеспечил информационную безопасность на все случаи жизни навсегда, и даже на долгий срок.

Следует иметь в виду, что даже правильно выстроенная на современном уровне система информационной безопасности компании не может обеспечить абсолютную защиту всех данных, программ и оборудования компании. Поэтому важно проводить постоянный, или по крайне мере, периодический, анализ рисков в сфере информационной безопасности для каждой компании отдельно. Во-первых, необходимо ранжировать информацию, и, соответственно, информационные систе-

мы и оборудование по степени важности для деятельности компании, обычно при этом исходят из оценок величины потерь, связанных с нарушением защиты каждого конкретного сегмента информационного пространства компании. Во-вторых, из всего спектра возможных угроз информационной безопасности необходимо выделить реальные на текущий момент, оценить вероятность каждой из них для каждого сегмента информационного пространства, а также сопоставимые величины потерь от их реализации. И только тогда по составленной карте рисков определять изменения в политике информационной безопасности.

Очевидно, что такую работу могут провести качественно только руководители достаточно высокого уровня, и на наш взгляд, глубоко ошибочным является подход, когда этим занимаются только специалисты по информационным технологиям. Конечно, они должны принимать участие в разработке политики информационной безопасности, и на них лежит полная ответственность за ее реализацию. Но разработка этой политики является зоной ответственности руководства компании.

При этом очень важно следовать принципам системного подхода, т. е. разработав комплекс мер безопасности для каждого сегмента информационного пространства, перейти к их синтезу на основе общей классификации угроз информационной безопасности.

Существуют три основных категории угроз:

- нарушение доступа;
- модификация;
- отказ в обслуживании.

Нарушение доступа — это попытка получения злоумышленником информации, для просмотра которой у него нет разрешений. Осуществление такой атаки возможно везде, где существует информация и средства для ее обработки.

Различают разные формы нарушения доступа:

1. Чтение. Может происходить либо через просмотр файлов или документов для поиска интересующей злоумышленника информации, либо через прослушивание при передаче данных. передачи Реализация этой угрозы имеет одну интересную особенность: информация не похищается, а копируется. Она остается у исходного владельца, но при этом ее получает и злоумышленник. Таким образом, владелец информации несет убытки, а обнаружить момент, когда это произошло, очень трудно.

2. Перехват. В отличие от прослушивания перехват — это активная атака. Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. После анализа информации он принимает решение о разрешении или запрете ее дальнейшего прохождения

Внедрение беспроводных сетей увеличило вероятность успешного прослушивания и перехвата. Теперь злоумышленнику не нужно нахо-

диться внутри системы или физически подключать подслушивающее устройство к сети. Вместо этого во время сеанса связи он располагается на стоянке для автомобилей или вблизи здания.

«Вочокинг» означает нанесение мелом специальных знаков на тротуарах около зданий офисов. Такие отметки сигнализируют взломщикам о точках входа в беспроводные сети компании.

Информационный доступ с использованием перехвата — одна из сложнейших задач для злоумышленника. Чтобы добиться успеха, он должен поместить свою систему в линии передачи между отправителем и получателем информации. В интернете это выполняется посредством изменения разрешения имени, в результате чего имя компьютера преобразуется в неправильный адрес, трафик перенаправляется к системе атакующего вместо реального узла назначения. При соответствующей настройке такой системы отправитель так и не узнает, что его информация не дошла до получателя.

Перехват возможен и во время действительного сеанса связи. Такой тип атаки лучше всего подходит для захвата интерактивного трафика типа telnet. В этом случае взломщик должен находиться в том же сегменте сети, где расположены клиент и сервер. Злоумышленник ждет, когда легальный пользователь откроет сессию на сервере, а затем с помощью специализированного программного обеспечения занимает сессию уже в процессе работы. Взломщик получает на сервере те же привилегии, что и пользователь.

Перехват более опасен, чем прослушивание, он означает направленную атаку против человека или организации.

3. Модификация. Атака модификации — это попытка неправомочного изменения информации посредством таких действий как замена, добавление и удаление.

Если взломщик уже имеет доступ к системе, такая операция оставляет после себя минимум улик. При отсутствии санкционированного доступа к файлам атакующий сначала должен обеспечить себе вход в систему или изменить параметры доступа через уязвимые места систем, например, «бреши» в безопасности сервера. Изменение файлов базы данных или списка транзакций требует высокой квалификации взломщика... В этих случаях необходимо основательно поработать во всей системе, чтобы воспрепятствовать обнаружению.

Модификации при передаче информации обычно выполняется в два этапа: сначала перехват интересующего трафика, а затем вносятся изменения в информацию перед ее отправкой к пункту назначения.

1. Отказ в обслуживании. Отказ в обслуживании реализуется через атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров.

2. Отказ в доступе к информации. Информация становится непригодной для использования: уничтожается, искажается или переносится в недоступное место.

3. Отказ в доступе к приложению. Решение задач, выполняемых с помощью такого приложения, становится невозможным.

4. Отказ в доступе к системе. Вся информационная система, установленные на ней приложения и вся сохраненная информация становится недоступной.

5. Отказ в доступе к средствам связи. Это наиболее распространенная угроза коммуникационной среде: это может быть разрыв сетевого провода, глушение радиопередач или лавинную рассылку сообщений, создающую непомерный трафик. При этом целостность отдельной компьютерной системы и информации не нарушается, однако отсутствие средств связи лишает доступа к этим ресурсам.

В заключение рассмотрим последовательность работ, которые должны регулярно выполняться, для обеспечения информационной безопасности компании (табл. 1).

Таблица 1

Последовательность работ для обеспечения информационной безопасности компании

	Виды работ	Исполнители
1.	Структурировать информационное пространство (ИП) компании, разбив его по возможности, на непересекающиеся сегменты.	Руководство компании
2.	Ранжировать эти сегменты ИП по важности	Руководство компании
3.	Для каждого сегмента ИП:	
3.1	Определить места формирования, обработки и хранения, а также пути передачи информации .	Руководство компании ИТ службы
3.2	Определить возможные угрозы для каждого	ИТ службы
3.3	Оценить вероятность для каждой угрозы по каждому.	ИТ службы
3.4	Ранжировать угрозы по полученной вероятности	ИТ службы
3.5	Разработать способы обнаружения и нейтрализации каждой угрозы.	ИТ службы
3.6	Оценить эффект каждого способа защиты	ИТ службы
3.7	Оценить затраты для каждого способа за-	ИТ службы

	щиты	
3.8	Сформировать вариант системы защиты с учетом вероятности угроз эффекта и затрат на способы их нейтрализации.	ИТ службы Руководство
4.	Интегрировать подготовленные варианты для отдельных сегментов ИП в единую систему информационной безопасности компании	Руководство ИТ службы

Информационная безопасность является необходимым условием успешной деятельности компании, но обеспечить ее абсолютно, раз и навсегда нельзя. Только постоянная совместная работа руководства компании и служб ИТ может поддерживать информационную безопасность компании на должном уровне.

Список литературы

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков — М.: Книжный мир, 2009. — 352 с.

2. Галатенко В. А. Стандарты информационной безопасности / В. А. Галатенко. — М.: Интернет-университет информационных технологий, 2006. — 328 с.: ил.

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — М.: ДМК Пресс, 2008. — 544 с.