ЭКСПЕРТНЫЙ СОВЕТ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И «СТРАШНЫЕ» ХАКЕРЫ

Роман Никишов,
компания «Дэт Норске Веритас» (DNV)

Информационная безопасность рассматривается, с одной стороны, как состояние защищённости информационной среды организации, а с другой стороны, представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Услышав слова «информационная безопасность», на ум сразу приходят страшные истории о проникновении всесильных хакеров в банковские системы, хищения миллионов долларов и прочие ужасы. Слов нет, эти случаи действительно имеют место. Как и достаточно нередкие (увы!) авиакатастрофы. Только число пострадавших на дорогах неизмеримо больше.

Аналогичная ситуация с информационной безопасностью. Хакерские атаки — это даже не вершина айсберга (1/8 от его массы). Ведь само понятие «информационная безопасность» распространяется, кроме конфиденциальности, ещё на целостность и доступность информации. А потери бизнеса от утраты данных или недоступности сервисов несопоставимы по значимости с последствиями хакерских взломов.

По данным опроса Computer Security Institute (USA), 43% американских компаний зафиксировали инциденты с информационной безопасностью. Средние финансовые потери на 1 респондента составили 288 618 дол. — весьма впечатляющая цифра. А по данным отчёта IT Policy Compliance Group, фирмы, уделяющие недостаточное внимание информационной безопасности, имеют каждый год более 80 часов простоя по вине отказов ИТ-сервисов, что приводит к уменьшению на 3% годового дохода. Совокупные же их финансовые потери от инцидентов с информационными технологиями (ИТ) оцениваются в 9,6 % этой величины.

ЭКСПЕРТНЫЙ СОВЕТ

Если учесть, что в области ИТ западные тенденции весьма быстро распространяются и в России, можно предположить серьёзность уровня данной проблемы.

3 кита информационной безопасности

В бытность свою системным администратором автор обслуживал одну небольшую компанию. Располагалась она в двух смежных гостиничных номерах, наскоро переоборудованных под офис. В работе случались перебои и со светом, и с телефонией. Встал вопрос о покупке блока бесперебойного питания (UPS). Директору компании были предложены на выбор 4 подходящие модели UPS.

Реакция директора была предсказуема: конечно, скажешь, что нужен самый дорогой? Однако встречный вопрос, сколько стоит восстановить данные за день работы фирмы, его несколько озадачил.

— А почему за день?

— Раз в день делается резервное копирование, по ночам. Так что если в результате отключения электричества данные на сервере пропадут, то надо будет восстановить все, что наработано с утра.

Звонок главбуху, в соседнюю комнату:

— Если у вас пропадут данные за рабочий день, как быстро вы их восстановите?

— В самом лучшем случае — за 3 дня.

Если сравнить трёхдневную зарплату главного бухгалтера, приплюсовав к ней суету, нервы и пр. эмоции, становится ясно, что даже самый дешёвый UPS, который годен только на то, чтобы корректно «погасить» сервер без потери данных, заведомо себя окупает.

А сколько стоит час простоя компании в «горячее время», того же главбуха в день перед сдачей отчёта? Более мощные и, соответственно, более дорогие модели позволят работать длительное время без выключения.

Этот пример хорошо иллюстрирует, что целостность и доступность данных не менее важны, чем конфиденциальность. А угроз для них может быть гораздо больше. Тут впору вспомнить заповедь африканских охотников: «Тот лев, которого вы видите, вас не убьёт. Вас убьёт тот лев, о котором вы не подозреваете».

Главное — система!

Целостность, доступность и конфиденциальность информации — это 3 «кита», на которых основывается информационная безопасность. Но чтобы в комплексе решать эти задачи, необходим системный подход и соответствующая система менеджмента, которая так и называется — система управления информационной безопасностью (СУИБ) или в английском оригинале — Information Security Management System (ISMS).

ЭКСПЕРТНЫЙ СОВЕТ

Такая система гарантирует, что составлен реестр всех информационных ресурсов (активов) организации, идентифицированы угрозы и риски, проанализированы уязвимые места и предложены меры воздействия.

Да, информационные технологии — довольно молодая бурно развивающаяся отрасль, поэтому риск—менеджмент является обязательной компонентой ее системы информационной безопасности. Особое внимание уделяется обеспечению непрерывности бизнеса и его составляющим — плану действий в чрезвычайных ситуациях и плану восстановления функционирования после сбоев.

Но будет ошибочным полагать, что возглавлять такую систему должен системный администратор или другой ИТ-«технарь». Еще Жан Жорес (1859—1914) задолго до У. Черчилля пропагандировал ту мысль, что «война есть слишком серьезное дело, чтобы поручать ее военным». ИТ-специалисты могут в одночасье придумать множество способов совершенствования системы (здесь и резервные дизель-генераторы, и трёхкратно дублированные интернет-коммуникации, и зеркальные дисковые массивы и т.д. и т.п.). Однако оценить истинную необходимость изменений и сделать оптимальный выбор можно, только опираясь на потребности бизнеса компании. Поэтому «шеф» информационной безопасности (chief information security officer) может не уметь настраивать, например, файрволы, его главная роль — быть медиатором, проводником между бизнес-подразделениями и узкоспециализированными ИТ-специалистами.

Не обязательно такая роль должна быть выделенной. Её с успехом сможет выполнять один из руководителей компании (в зависимости от масштаба бизнеса). Главное — чтобы эти аспекты в принципе не остались без внимания, чтобы вопрос, «сколько стоит час простоя компании?», гарантированно прозвучал хотя бы в одной «ответственной голове».

СПРАВКА

Файрвол

(файрво́лл, файерво́л, фаерво́л — от англ. firewall) — межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

http://ru.wikipedia.org/

«Киты» в облаках

Информационная безопасность важна внутри компании, но не менее серьёзна она для внешних сервисов. Задумайтесь, скольким внешним контрагентам мы вверяем свои данные. Сейчас особенно модны «облачные» технологии. Однако насколько хорошо «киты» информационной безопасности чувствуют себя в этих «облаках»? Ведь, несмотря на абстрактность понятия «облако», данные хранятся на вполне конкретном сервере вполне конкретного датацентра. Насколько этот датацентр способен обеспечить те самые конфиденциальность, целостность

и доступность? Написано что-то про это в договоре с ним (если такой договор вообще существует)? Определены ли там гарантированные уровни сервиса (Service Level Agreemant, SLA)?

А партнёры и контрагенты компании? Имеется уверенность, что они способны надёжно защитить данные, которые им передают? Ведь письма электронной почты идут через ряд промежуточных серверов, и администратор любого из них может спокойно читать всю корреспонденцию (если она не зашифрована). Каждый интернет-провайдер досконально знает, какие сайты посещают сотрудники компании, на каких страницах задерживаются, и какие запросы в Яндексе набирают.

СПРАВКА

Service Level Agreement (SLA) — соглашение об уровне предоставления услуги, содержащее описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной услуги.

http://ru.wikipedia.org/

Чтобы избежать всех этих неприятностей, существует сертификация по стандарту информационной безопасности ISO 27001. Этот стандарт описывает требования к системе менеджмента информационной безопасности компании. В «довесок» к нему идут ещё около 10 стандартов, описывающих разные аспекты менеджмента информационной безопасности (риск-менеджмент, конкретные методы защиты и т.д.). Сертификация по этому стандарту добровольная, обычно право проводить её (аккредитацию) имеют те же органы, что проводят сертификацию по стандартам системы менеджмента качества (ISO 9001), экологической безопасности (ISO 14001) и т.д.

Стандарт 27001 ещё не так широко распространён в России, но в мире занимает весьма почётное 5 место с результатом 15625 выпущенных сертификатов (на конец 2010 г.). Конечно, он сильно отстаёт по этому показателю от стандартов «большой тройки» — уже упомянутые ISO 9001 (более чем 1 млн 100 тыс. сертификатов), ISO 14001 (около 250 тыс. сертификатов) и стандарт качества в автомобильной промышленности ISO/TS 16949:2009 (около 44 тыс.), но «дышит в спину» ближайшему соседу — стандарту качества на медицинское оборудование ISO 13485:2003 (18834 сертификатов).

И это не удивительно. Ведь наличие стандарта 27001 гарантирует, что обладающая им компания имеет внедрённую систему информационной безопасности, поэтому может на адекватном уровне поддерживать те самые конфиденциальность, целостность и доступность данных, находящихся под её управлением. Такая гарантия становится всё более востребованной.