Внутренние против внешних

Как бороться с угрозами потери данных

На фоне борьбы против компьютерных злоумышленников идёт и борьба между разными технологиями и средствами защиты информации. Лишь в минуту настоящей опасности все конкуренты перестают тянуть одеяло на себя и объединяются для защиты информационных ресурсов.

Николай ФЕДОТОВ,
главный аналитик компании InfoWatch

Профессионалы в области защиты информации давно делят все угрозы на внутренние и внешние — в зависимости от того, по какую сторону сетевого шлюза расположен потенциальный злоумышленник. До недавних пор внешние были популярнее: их боялись, их обсуждали, про них писали в прессе и снимали фильмы в Голливуде, против них покупали средства защиты. Потом мода изменилась. Видя, что рынок насыщается и продавать межсетевые экраны становится всё труднее, производители затянули новую песню и стали «популяризировать» угрозы внутренние. В прессе всё чаще поминаются инсайдеры, разглашающие коммерческую тайну, высшие менеджеры, теряющие ноутбуки с критически важной информацией, промышленные шпионы, внедряющиеся к конкурентам, и т. п.

Но не спешите обвинять производителей в алчности и манипуляциях. Информационная безопасность сейчас явно недооценена. На неё затрачивается порядка 2–3% бюджета на все информационные технологии, а во многих российских организациях — и того меньше. В то время как соотношение аналогичных затрат на функционирование бизнеса и на его безопасность в мире значительно выше и достигает 10%.

Недаром во время последнего финансового кризиса в 2009 году отрасль информационной безопасности пострадала меньше других. Например, мы, компания InfoWatch, почувствовали это, так сказать, на собственной шкуре. Под давлением обстоятельств руководители предприятий сокращали всё, без чего могли обойтись: лишний персонал, лишние площади, лишнюю рекламу. Но лишней безопасности им отыскать не удалось. Бюджеты на ИБ подверглись наименьшему урезанию: меньше, наверное, пострадали только премии высших менеджеров. Число заказов у нас почти не снизилось, разве что замедлилось поступление платежей. Но в первом квартале 2010-го всё уже восстановилось.

Это ещё раз подтверждает, что ИБ была недооценена. Расходы на неё меньше сокращались. И расходы на неё будут расти.

Что интересует хакера?

Распределяя деньги на защиту от внешних угроз, надо понять логику противника и для этого думать не как защитник, а как злоумышленник. Самая толстая броня у танка — не там, где самые важные части, и тем более не там, где самые дорогие. Наибольшая толщина брони — в тех местах, куда чаще попадают. Информационное бронирование следует строить по тому же принципу.

Распространённой ошибкой является выделение наибольшего бюджета на защиту той информации, которая представляется наиболее ценной с точки зрения руководителя (владельца) предприятия. Практика показывает, что хакеры мало интересуются грязным бельём босса фирмы. Они направляют атаки на такую информацию, которую можно побыстрее и подороже продать (табл. 1). Ни бухгалтерский баланс, ни списки клиентов российских предприятий на чёрном рынке не котируются. Зато быстро уходят пароли от электронной почты, ICQ и соцсетей, учётные записи на взломанных серверах. А лучше всего — номера банковских

Таблица 1

Распределение утечек по типам конфиденциальных данных

Тип конфиденциальных данных	1-е полугодие 2009 года		1-е полугодие 2010 года	
	Кол-во	%	Кол-во	%
Персональные данные	360	87,2	374	97,9
Коммерческая тайна, ноу-хау	12	2,9	2	0,5
Государственная и военная тайна	9	2,2	2	0,5
Другая конфиденциальная информация	28	6,8	4	1,0
Не установлено	4	1,0	0	0

Таблица 2

Основные каналы утечки данных

Канал утечки	1-е полугодие 2009 года		1-е полугодие 2010 года	
	Кол-во	%	Кол-во	%
Мобильный компьютер (ноутбук, КПК)	49	11,9	40	10,5
Мобильный носитель (USB-Flash, CD, DVD и т. п.)	23	5,6	32	8,4
Настольный компьютер, сервер, жёсткий диск	41	9,9	90	23,6
Интернет (в том числе эл. почта)	97	23,5	82	21,4
Бумажный документ	84	20,3	78	20,4
Архивный носитель	48	11,6	6	1,6
Другой	36	8,7	25	6,5
Не установлено	35	8,5	29	7,6

карт. Особо ценным (хотя и особо редким) товаром на чёрном рынке является доступ к клиентской программе по управлению банковским счётом («клиент-банк»): как правило, такой доступ осуществляется через внедрение троянской программы на соответствующий бухгалтерский компьютер.

Вот те ресурсы, которые внешний противник постарается захватить при атаке на вашу систему. Всё остальное ему просто не нужно, поэтому на защиту от соответствующих угроз надо оставить разумный минимум. А основные средства сосредоточить для защиты наиболее ценных — не для вас, а для них — ресурсов.

Загадка изнутри

С внутренними угрозами бороться сложнее, потому что их источник — мы сами. Люди, с которыми каждый день приходишь в один офис и делаешь одно дело. Друзья и коллеги. Даже местный сисадмин и безопасник тоже рассматриваются как потенциальные злоумышленники. И их предлагается считать источником опасности? Им — не доверять, проверять их и отслеживать? Делать такое тяжело в моральном плане. Но технически и организационно все нужные решения и схемы давно разработаны.

Возможно, кого-то утешит мысль, что внутренний «злоумышленник» — это не обязательно человек и не обязательно замышляющий что-то нехорошее. Например, поступила информация, что с вашего офисного IP-адреса зафиксирован спам, вредоносный трафик или атака на чужой компьютер. Это может означать, что:

- с вероятностью 90% один из ваших компьютеров подхватил какого-то сетевого паразита, и теперь им управляет вредоносная программа или неизвестный злоумышленник использует в качестве посредника;
- с вероятностью 9% ваш IP-адрес подделан злоумышленником, и атакуемый добросовестно заблуждается, обвиняя вас;
- с вероятностью 0,9% кто-то из работников действительно творит нечто нехорошее.

Тем не менее это всё тоже внутренние угрозы. Меры противодействия тут играют роль второго эшелона обороны. Если враг прорвал внешнюю защиту, у вас должен быть второй шанс выявить и остановить атаку.

Немного об утечках

Отдельная категория внутренних угроз — утечки информации. Как ни странно, большинство (хотя и не подавляющее — от 50 до 75%) утечек являются случайными и происходят по разгильдяйству, лени или невнимательности своих же работников (табл. 2 и 3). Намеренные утечки также в большинстве случаев можно свалить на собственный персонал, который нарушил политику безопасности и «не предотвратил», «не сберёг», «не обратил внимания». Зачастую утечку вообще невозможно классифицировать, т. е. уверенно сказать про неё, намеренная она или случайная.

Типичнейший и массовый случай: **внезапно** у руководителя пропал ноутбук. То ли потерял, то ли украли. То ли вор (или нашедший) реализует его как материальную ценность, то ли станет пытаться извлечь выгоду из конфиденциальной информации на диске. Большинство воров, даже самых «низкоуровневых», уже в курсе, что информация из ноутбука, смартфона или флешки может стоить в разы больше, чем её носитель. Подобный инцидент однозначно должен быть отнесён к внутренним угрозам, поскольку пользователь (или сисадмин) должен был учитывать такой риск и зашиф-

Таблица 3

Каналы утечки для случайных и намеренных инцидентов

Канал утечки	Случайные		Намеренные	
	Кол-во	%	Кол-во	%
Мобильный компьютер (ноутбук, КПК)	11	5,9	23	13,6
Мобильный носитель (USB-Flash, CD, DVD и т. п.)	18	9,7	12	7,1
Настольный компьютер, сервер, жёсткий диск	23	12,4	61	36,1
Интернет (в том числе эл. почта)	58	31,4	23	13,6
Бумажный документ	62	33,5	14	8,3
Архивный носитель	2	1,1	2	1,2
Другой	7	3,8	16	9,5
Не установлено	4	2,2	18	10,7

ровать все данные на мобильном устройстве. Утрата зашифрованного носителя инцидентом вообще не считается, ибо современная гражданская криптография совершенно спокойно противостоит не то что ворам, а и спецслужбам вероятного противника со всеми их суперкомпьютерами.

Учёт и контроль

Ну и апофеоз борьбы с внутренним злом — это внедрение так называемой DLP-системы. Она контролирует все каналы передачи информации через защищаемый периметр: сетевой шлюз, принтер, запись на CD и т. п., на флешки и другие отчуждаемые накопители. Вся пересекающая периметр информация проверяется в реальном времени на предмет наличия в ней конфиденциальных сведений (рис. 1 и 2). При этом DLP «заглядывает внутрь» архивов, расшифровывает то, что зашифровано, распознаёт разные форматы данных, переводит с иностранных языков, ищет стеганографию (размещение секретного файла внутри обычного, например мультимедийного). Всё, что содержит конфиденциальную информацию или не поддаётся расшифровке, блокирует. А всё прошедшее через границу на всякий случай сохраняет в архив — для возможных в будущем расследований.

Понятно, что DLP — вещь очень дорогая и создающая массу неудобств до тех пор, пока не приучит работников к порядку. Или пока они не приучат её к традиционному бардаку — это уж как доведётся.

Например, была такая история. Внедряли на предприятии электронный документооборот. Каждый из документов, циркулирующих в системе, должен иметь совокупность меток доступа: каким пользователям и группам какие действия разрешены над соответствующим документом. Работников — сотни, документов — тысячи, причём каждый день новые тысячи. Разумеется, невозможно поручить расстановку меток доступа одному человеку или группе, поскольку для этого необходимо разбираться в сути, в содержании документа, в описываемых процессах, а такими широкими знаниями никто не обладает. Естественно, расстановка должных привилегий в каждом новом документе была поручена его создателю: он сам должен был решить, кому можно это читать, кому править, кому копировать, кому отправлять по внешним адресам и т. д. Сначала все честно пытались выполнить требования инструкции. Но вскоре поняли, что предвидеть будущее нелегко и ошибок избежать не удаётся. То запамятовал включить кого-то нужного в список допущенных, то забыл дать право редактирования собственному начальнику, то срок доступа выставил неверный. По каждой такой ошибке — выяснения, ходатайства, запросы на изменение, обиды, жалобы и нагоняи. Вскоре все работники сделали совершенно логичный вывод: чтобы избежать проблем, надо ставить во всех документах максимально широкие полномочия, когда «всем можно всё». Найденное народом «решение» немедленно подтвердило

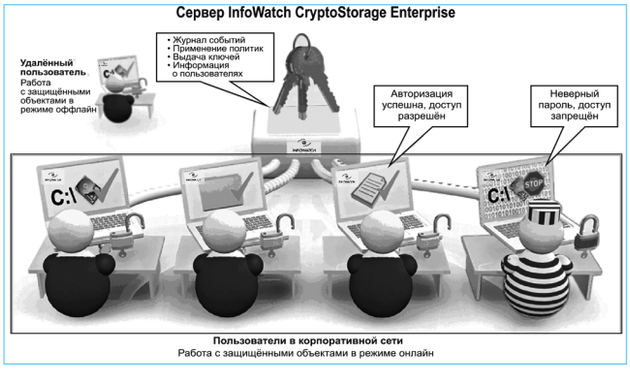

Рис. 1

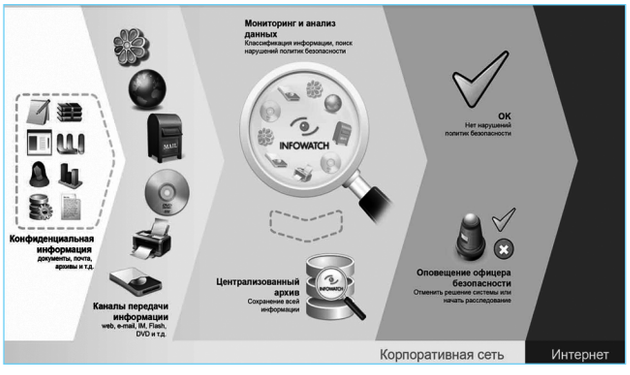

Рис. 2

свою эффективность: проблемы закончились. А установленная защита от утечек оказалась бессмысленной тратой времени и денег.

Бывали и другие случаи, когда внедрение системы защиты от утечек заканчивалось неудачей. И ещё хорошо, если об этой неудаче честно докладывали начальству: тогда можно было извлечь уроки и прекратить бесполезные издержки. Но бывало, что докладывали об успехе. Это ещё худший вариант. Как известно, полное отсутствие защиты лучше, чем неработающая защита, поскольку не возникает неоправданных надежд.

Заключение

Чтобы поделить ваши ограниченные ресурсы между защитой от внешних и от внутренних угроз (табл. 4), следует оценить их вероятность и возможный ущерб (их произведение высоконаучно именуется стоимостью риска). Высчитать эту стоимость не всегда получается даже приблизительно.

Но уж точно не стоит применять такой метод оценки, как восприятие аргументов заинтересованных сторон — продавца очередного средства защиты и представителя подразделения информационной безопасности. Первый склонен продать как можно больше товара, второй желает получить как можно больше привилегий. Оценку рисков должна проводить незаинтересованная сторона. Например, финансовый департамент.

Таблица 4

Технические средства защиты

Против внешних угроз	Против внутренних угроз
— межсетевой экран (Firewall); — антивирус на почтовом сервере; — антиспамовая система; — шифрование трафика (VPN); — ханипот (ложная цель, на которую злоумышленник зря тратит свои ресурсы)	— антивирус на рабочей станции; — система разграничения доступа; — виртуальные машины и среды; — системы предотвращения мошенничества: антифрод (Antifraud), FPS (Fraud protection systems); — DLP-система
Против обоих видов угроз	
— резервное копирование (Backup); — обнаружение вторжений (IDS (Intrusion Detection System), IDP (Intrusion Detection Protection) — системы выявления и предотвращения вторжений); — авторизация, аутентификация и учёт (AAA)	

На самый часто задаваемый вопрос, какие угрозы опаснее — внутренние или внешние, всё время подмывает процитировать Сталина. Когда перед ним поставили сходный вопрос, какой уклон хуже — правый или левый, он, понимая, что политическим противникам нельзя давать поблажки ни в чём, ответил: «Оба хуже!». Фраза стала крылатой.