ВРАГ У ВОРОТ

В 2007 ГОДУ, СОГЛАСНО ПРОГНОЗАМ, СОВОКУПНЫЙ ОБЪЕМ ПРОДАЖ ПО ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОЛЖЕН БЫЛ ВПЛОТНУЮ ПРИБЛИЗИТЬСЯ К МИЛЛИАРДУ ДОЛЛАРОВ, А В 2008-М — ПЕРЕШАГНУТЬ МИЛЛИАРДНУЮ ОТМЕТКУ. ПРЕДПОСЫЛКИ К ЭТОМУ ОЧЕВИДНЫ УЖЕ СЕЙЧАС. ПОТОМУ ЧТО ПОТЕРИ КОМПАНИЙ СЛИШКОМ ВЕЛИКИ, ПРИЧЕМ НЕ ТОЛЬКО ОТ ВНЕШНИХ АТАК, НО И ПО ПРИЧИНЕ ВНУТРЕННИХ УТЕЧЕК, И ОСОБЕННО В РЕЗУЛЬТАТЕ ИНСАЙДЕРСКИХ ПРЕСТУПЛЕНИЙ. ГРИГОРИЙ РУДНИЦКИЙ, АЛЕКСЕЙ ДОЛЯ

ЗАЩИТА ОТ ИНСАЙДЕРА Осенью 2007 года были опубликованы результаты исследования «Global Economic Crime Survey 2007», проведенного компанией PricewaterhouseCoopers (одной из крупнейших аудиторских фирм в мире, предоставляющей услуги в области бизнес-консультирования, налогообложения и права). В нем приняли участие 5400 компаний из 40 стран, включая 125 ведущих российских компаний. Оно показало, что за последние два года с экономическими преступлениями, вызванными нарушением режима информационной безопасности внутри компаний, столкнулось большинство респондентов.

При этом виновными в большинстве случаев оказывались топ-менеджеры, а средний материальный ущерб от мошеннических действий составил $12,8 млн. Лидером по числу инсайдерских преступлений стала Россия: более половины (59%) российских компаний пострадали за последние два года как минимум от одного серьезного экономического преступления. Этот показатель на 10% превышает число выявленных в России в ходе обзора 2005 года, а также значительно выше среднемирового (43%) и среднеевропейского (50%) уровней.

В основном это были хищения активов компании, нарушения прав интеллектуальной собственности (в том числе утечка информации, составляющей коммерческую тайну), искажения отчетности. Не стоит забывать и о косвенном ущербе — потере репутации, судебных разбирательствах и падении морального духа компании. На это же указывают в своем отчете эксперты PwC: 67% российских пострадавших компаний понесли косвенные убытки. Однако эксперты компании Perimetrix, занимающейся защитой от утечек информации, убеждены, что доля косвенного ущерба российских компаний невелика по сравнению с общим масштабом убытков. Дело в том, что в отечественном бизнесе все еще бытует мнение, что любые инсайдерские преступления нельзя предавать огласке: чаще всего виновного втихую увольняют, а службу безопасности лишают премии.

При этом 31% пострадавших российских респондентов ответили, что в их компании работает более 5000 сотрудников. Как показывает исследование, от мошенничества страдают и крупные, и небольшие компании. По мнению экспертов компании Perimetrix, виной тому — неэффективная работа систем информационной безопасности, которые никак не регламентируют доступ к конфиденциальным данным. При этом, чем крупнее компания и ее штат, тем больше у нее уязвимых мест, а соответственно больше убытки.

Исследование показало, что исполнителями почти половины инсайдерских преступлений были топ-менеджеры компании, а заказчиками — конкуренты или деловые партнеры. Как отмечается в отчете PwC, все большее число инцидентов совершается штатными сотрудниками компании (38% в 2007 году против 13% в 2005 году). Настораживает тот факт, что 41% преступников внутри российских предприятий занимают руководящие посты. Этот показатель, по данным опроса, значительно выше, чем в странах Центральной и Восточной Европы (38%) и в остальных странах мира (20%). Эксперты Perimetrix объясняют это тем, что руководство лучше знает сильные и слабые стороны компании. Топ-менеджмент компании, имея полный доступ к финансовым и информационным активам, прекрасно знает все ее наиболее уязвимые места. Служебное положение дает возможность закамуфлировать свои действия и принятые в ущерб интересам собственника решения.

Самым распространенным видом преступлений в сфере внутренней безопасности в странах Центральной и Восточной Европы является незаконное присвоение или хищение корпоративных активов (43%). Далее следуют нарушение прав интеллектуальной собственности и искажение отчетности (28% и 18% соответственно). По оценкам экспертов Perimetrix, из-за внутренних преступлений компании теряют около 2% своего оборота.

Еще один факт: 67% российских компаний за последние два года потеряли не одну сотню миллионов долларов в результате действий инсайдеров. Затраты на устранение косвенного ущерба составили около $110 млн. Предотвратить инсайдерскую утечку данных могут вовремя принятые меры. Обнаружить попытку мошенничества можно тремя способами: случайным образом, работой механизма внутреннего контроля и с помощью аудита. Большинство экономических преступлений в России были раскрыты корпоративной службой безопасности и службой внутреннего аудита (28% и 20% соответственно). Динамика обнадеживает: в 2005 году подавляющее большинство случаев мошенничества было выявлено случайно (35% в 2005 году и 21% в 2007 году), а служба внутреннего аудита участвовала в выявлении лишь 7% противоправных действий.

Почти все российские респонденты (98%) заявили, что уже принимают меры по предотвращению мошеннических действий. 24% российских компаний, участвовавших в опросе, внедрили новые способы контроля, а 37% предприятий в последние два года усилили существующие меры контроля, осознав, что гораздо выгоднее потратиться на предотвращение инсайдерских преступлений, чем каждый год списывать миллионы долларов по статье «незапланированные расходы».

PwC в своем отчете нарисовала портрет типичного информационного мошенника: мужчина в возрасте от 31 года до 40 лет с высшим образованием, находящийся на руководящей должности около двух лет.

ПОРТРЕТ ТИПИЧНОГО ИНФОРМАЦИОННОГО МОШЕННИКА: МУЖЧИНА В ВОЗРАСТЕ ОТ 31 ГОДА ДО 40 ЛЕТ С ВЫСШИМ ОБРАЗОВАНИЕМ, НАХОДЯЩИЙСЯ НА РУКОВОДЯЩЕЙ ДОЛЖНОСТИ ОКОЛО ДВУХ ЛЕТ

ВАЛЕРИЙ МЕЛЬНИКОВ

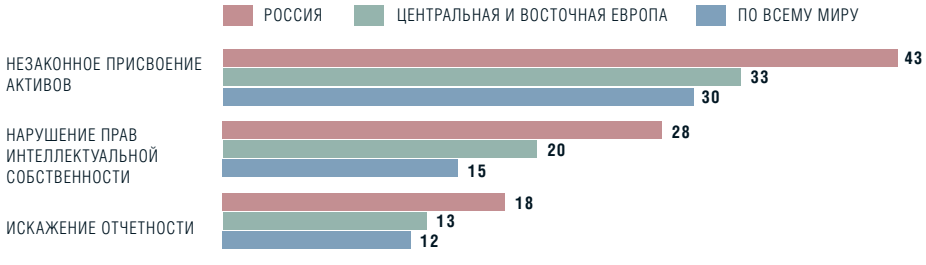
ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Согласно ежегодному отчету ведущей организации безопасности SANS Institute, слабейшим звеном в любой системе защиты по-прежнему являются пользователи, то есть человеческий фактор.

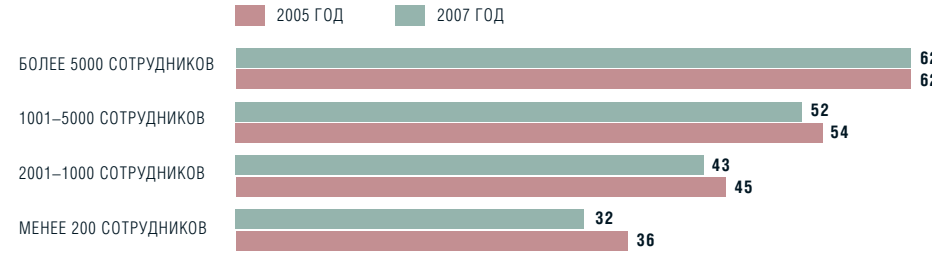
Около 52% опрошенных пользуются корпоративной электронной почтой из гостиниц, аэропортов и интернет-кафе. Еще большее число респондентов забирает рабочую почту из точек доступа беспроводных сетей. 63% опрошенных часто отправляют рабочие документы на свой личный e-mail, чтобы иметь возможность работать с ними вечером дома. Наконец, около 8% участников опроса признались, что когда-либо теряли ноутбук, флэш-диск или смартфон с корпоративной информацией.

Причина, по которой работники пренебрегают служебной безопасностью, предсказуема: они считают правила неудобными и малопонятными. Поэтому около 35% сотрудников приходится нарушать их для выполнения своей работы. Поэтому при разработке правил ИТ-безопасности следует учитывать реалии человеческого поведения. И, разумеется, не пренебрегать обучением пользователей.

ЗАЩИТА ОТ ДУРАКА «Раньше даже крупные российские компании подходили к охране своей информации фрагментарно, внедряя отдельные продукты и не имя при этом четкого плана и стратегии защиты. Исключение, пожалуй, составляли только банки и другие финансовые учреждения. Сейчас ситуация меняется кардинально — все больше предприятий разрабатывает комплексные меры защиты информации»,— отмечает старший маркетинговый аналитик «Лаборатории Касперского» Олег Гудилин.



РЕАЛЬНЫЕ СЛУЧАИ МОШЕННИЧЕСТВА В СФЕРЕ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (%)
ИСТОЧНИК: PWC, 2007 ГОД.



ЧЕМ БОЛЬШЕ КОМПАНИЯ, ТЕМ БОЛЬШЕ УБЫТКИ ОТ ИНСАЙДЕРОВ (%)
ИСТОЧНИК: PWC, 2007 ГОД.