Риски утечки информации

написано Александр Астахов | 10 июня, 2023

Для иллюстрации кибер-угроз в предыдущих раздел использовались инциденты, происходившие в последние годы в США. Однако все сказанное относится и к России, которая, в отличие от США, в меньшей степени подвержена кибер-угрозам, благодаря значительно меньшей степени интеграции в кибер-пространство.

Зато одной из серьезнейших проблем нашего государства, с которой по объективным причинам очень сложно бороться, является утечка конфиденциальной информации. Служебная, банковская тайна, персональные данные граждан во многих случаях становятся общедоступной информацией. Банковские проводки из расчетных центров, базы данных налоговой инспекции, ГИБДД, абонентов сетей сотовой и фиксированной связи, а также многое другое можно найти в широкой продаже по доступным ценам. Продажа украденных через Интернет номеров кредитных карт является активно развивающимся криминальным бизнесом. Такая ситуация помимо того, что приводит к катастрофическим последствиям для отдельных организаций и граждан, оказывает очень плохое влияние на развитие в стране экономической, правоохранительной и налоговой систем, повышает уровень террористической угрозы, снижает уровень защищенности общества в целом.

Несмотря на то что раскрытие информации является во многих случаях административно и уголовно наказуемым деянием, в условиях, когда информационное законодательство еще не полностью сформировано и существенно отстает от уровня развития информационных технологий, возникают существенные трудности с защитой интересов собственника информации.

Если не брать административной и уголовной ответственности отдельных граждан за разглашение персональных данных или коммерческой тайны (такая практика в нашей стране еще только начинает складываться), утечка информации часто приводит к

косвенному ущербу, такому как потеря конкурентных преимуществ или упущенная выгода, не поддающемуся точной финансовой оценке. Например, разглашение стратегических планов компании или определенных финансовых показателей. Это напоминает ущерб от скрытой болезни человека, глубоко сидящей в организме и с трудом поддающейся диагностированию и лечению. Эта болезнь постепенно подтачивает здоровье и приводит к снижению эффективности деятельности. Иногда случаются обострения, как в случае с компанием Victoria Secrets, которая была оштрафована в США на $50000 за то, что не обеспечила надлежащей защиты своего Web-сайта электронной коммерции, в результате чего пострадали 560 клиентов, счета которых оказались скомпрометированными.

Раскрытие внутренней информации о планируемых кадровых перестановках или уровне заработной платы работников может привести к ухудшению морального климата в коллективе, поэтому многие компании охраняют такую информацию, как самую большую тайну, за разглашение которой следует немедленное увольнение.

Отрывок из статьи Джон Кейс «Когда зарплата уже не секрет»:

Никто в компании не думал, что уволившаяся Триси способна на козни… В тот день, когда она должна была покинуть компанию, девица взломала базу данных службы по работе с персоналом и разослала по внутренней сети сведения о размере зарплаты всех сотрудников. Теперь каждый сотрудник знает, какая зарплата у всех остальных, и в компании царит настоящий хаос. Часть сотрудников в ярости оттого, что получает меньше других, а остальные испытывают неловкость, что получают намного больше.

Не вдаваясь в дискуссию относительно достоинств и недостатков закрытых систем оплаты труда, следует признать, что такие системы и связанная с ними угроза раскрытия конфиденциальной информации о зарплатах сотрудников являются реальностью для

многих организаций. Не менее значимой реальностью является незащищенность персональных данных.

_____

2005: Разгром ChoicePoint

ChoicePoint, один из крупнейших накопителей данных и реселлеров в США, объявил, что мошенники смогли получить доступ к базе данных, содержащей информацию о 145000 потребителей. Компания была не в состоянии полностью идентифицировать частные лица и организации, купившие эту информацию, включая личные дела и номера социального страхования.

_____

Инцидент с ChoicePoint стал главным событием, которое переместило акцент с хакерства на опасные бизнес-процессы и привело к увеличению регулирования в области защиты данных потребителя. В то время Калифорния была единственным штатом, в котором существовал закон об уведомлении о нарушении безопасности данных SB 1386, который заслужил всеобщее внимание после инцидента с ChoicePoint. Это событие дало толчок почти всем современным требованиям в области шифрования. На сегодняшний день 38 штатов в США имеют законы по раскрытию данных для общественности. Это также побудило федеральную комиссию по торговле наложить наибольший на тот момент штраф – ChoicePoint был обязан выплатить 15 миллионов долларов по обвинению в том, что компаниянарушила права на частную жизнь и была не в состоянии защитить информацию о клиентах.

В 2007 году произошла крупнейшая утечка данных в финансовой сфере. Американский розничный гигант TJXобъявил, что данные около 100 млн. его клиентов были похищены. Хакеры проникли в беспроводную сеть компании и получили доступ к данным, передаваемым между переносными наладонными устройствами, считывающими цену, компьютерами магазина и кассовыми

аппаратами. TJX критиковали за сбор избыточной информации, ее слишком необоснованно долгое хранение, и за то, что он был не в состоянии улучшить безопасность своей беспроводной сети, перейдя от WEP-протокола шифрования (старый стандарт) к WPA (который намного более надежен). TJX также подвергся нападкам, за то, что слишком долго скрывал информацию о данном инциденте и не обеспечил несоответствие стандартам безопасности данных индустрии платежных карт (PCI DSS). По оценкам некоторых экспертов, убытки TJXв результате данного инцидента составили более $1 млрд.

Спустя год в Великобритании произошла еще одна крупная утечка персональных данных. Почти половина населения этой страны оказалась «засвеченной» по вине налоговиков.

_____

В 2008 году председатель департамента налоговых и таможенных сборов Великобритании Пол Грей покинул свой пост после того, как его служащими были потеряны диски, содержащие информацию о 7,5 миллионах семей (25 миллионов человек), подавших заявления на получение детских льгот. Потерянные данные включалив себя имена, адреса, банковскую информацию, номера страховых полисов и другую персональную информацию. Речь идет почти о половине 60-миллионного населения Великобритании. Насколько нам известно, потерянные данные не были зашифрованы.

_____

Упомянутые выше инциденты – только верхушка айсберга. Ежедневно в СМИ публикуются десятки сообщений о крупных утечках. Неужели ничего не делается для защиты информации? Если глубже разбираться в описанных ситуациях, то выясняется, что защитные меры обычно принимаются, стандартам организации следуют, деньги на безопасность тратятся. Непонятно только одно – кто и каким образом оценивает риски утечки информации. В результате получается, что либо какие-то угрозы недооценили, либо вообще защищали не те данные и не от тех угроз.