Угрозы из сети

В вопросах информационной безопасности многие ритейлеры привыкли полагаться на авось и стараются максимально сэкономить деньги компании, поскольку возврат инвестиций в ИБ подсчитать практически невозможно. Однако недооценка угроз может привести к очень серьезным потерям. К примеру, конфиденциальная информация о ценовых предложениях поставщиков, условиях поставки товаров, планируемых к открытию торговых точках, попав в руки конкурентов, может значительно ослабить положение компании на рынке. В ближайшее время угрозы будут возрастать, так как в кризис теневой хакерский бизнес становится только крепче.

АВТОР: Наталья Николаева

Отчеты профильных организаций утверждают, что уровень угроз растет, а вот качество защищенности в корпоративном секторе, если сравнивать с 2011–2012 годами, наоборот, падает. Так, Positive Technologies в своем «Сборнике исследований по практической безопасности» за 2014 год заявила, что 86% исследованных ими в 2013 году корпоративных информационных систем имеют уязвимости, с помощью которых можно получить полный контроль над всеми критически важными для компании программами. Почта, ERP-система, системы управления сетевым оборудованием – все окажется в руках злоумышленника, если он знает, за какие ниточки дергать. И это еще не самое страшное! Иногда и особых знаний не требуется. По данным той же компании, если брать внутренние сети, то в «половине всех исследованных систем успешные атаки возможны со стороны любого неквалифицированного пользователя внутренней сети».

Это вроде как в теории и при тестовых проникновениях в сеть аудиторов по информационной безопасности. А что на практике? На практике то же самое. В конце ноября 2014 года хакеры успешно взломали сеть и парализовали работу ни много ни мало всемирно известной Sony Pictures Entertainment – организации солидной и с деньгами. Достоянием общественности стали внутренняя отчетность компании, сведения о сотрудниках: например, данные по зарплатам топ-менеджмента, а также такие личные данные, как номера карт социального страхования, зная которые, можно украсть у их владельцев если не все, то многое.

«Думаю, из этой истории можно сделать несколько выводов, – размышляет Сергей Хайрук, аналитик компании InfoWatch. – Во-первых, этот инцидент развенчивает миф о том, что кибератака, внутренняя или внешняя, несет в себе только угрозу репутации компании, но едва ли приведет к реальному финансовому ущербу. Как нам известно, взлом Sony Pictures Entertainment повлек за собой утечку четырех новейших фильмов, еще не вышедших в прокат. Судите сами, сколько компания потеряла на этом. Во-вторых, представители ФБР утверждают, что такая крупномасштабная операция не могла быть успешно осуществлена без помощи «крота» в самой корпорации. То есть даже в этой, казалось бы, внешней хакерской атаке был задействован бывший или действующий сотрудник Sony Pictures Entertainment, причем, по мнению ФБР, довольно высокого ранга. Это доказывает, что злонамеренные действия внутреннего сотрудника могут быть очень ощутимыми для компании, и на эти так называемые внутренние риски нельзя смотреть сквозь пальцы».

Забавный момент: СМИ опубликовали оставленную на взломанных хакерами компьютерах Sony Pictures картинку, содержащую текстовые угрозы и гиперссылки на архивы с некоторыми украденными данными. Западные масс-медиа эти ссылки прикрыли «блюром», что ничуть не помешало нашим журналистам раздобыть такую же картинку со всеми ссылками без какой-либо «занавески» и в таком виде поместить изображение в свои статьи об инциденте. Вот вам и «безопасность».

«Выводы тут самые простые, – говорит Станислав Шевченко, технический директор компании SafenSoft. – Даже такие крупные компании, которые однозначно уделяют безопасности не последнее место в своем бизнесе, подвергаются успешным атакам. В списке целей киберпреступников каждая компания может найти свое место».

Пока писалась эта статья, пришла еще одна интересная новость, отечественного розлива: вполне добропорядочный гражданин, не чуждый мира ИТ, случайно, но с небольшой помощью соцсети «ВКонтакте» (!) получил доступ к более чем 20 000 московских камер наблюдения и сообщил об этом в Единый центр хранения данных Москвы – государственную информационную систему, которой и принадлежит это хозяйство. Ответной реакции он дождаться так и не смог, зато опубликовал информацию на крупнейшей ИТ-площадке, так что теперь любой желающий мог убедиться в том, что уязвимость присутствует, что все и проделали. После бурного обсуждения в комментариях появился наконец представитель Департамента информационных технологий города Москвы и разъяснил присутствующим, что никакой утечки информации не было, просто сервис тестируют. Однако доступ к камерам тут же прикрыли.

В БАГДАДЕ ВСЕ СПОКОЙНО...

Но вернемся к бизнесу. На первый взгляд, дела у нас обстоят не так плохо, как на Западе. Никакой русский Эдвард Сноуден (которого, кстати, в западных СМИ зовут whistle-blower – доносчик) не бежит в США с нашими секретами, особенно громких скандалов, связанных с утечками информации, не наблюдается и в отечественных корпорациях. Но если мы о чем-то не знаем, это не значит, что явления нет. «К сожалению, в России компании не обязаны раскрывать информацию об утечках, уведомлять уполномоченные органы или своих клиентов в случае компрометации их данных», – сетует Сергей Хайрук. По его словам, число