Согласно ежегодному отчету Sophos о кибербезопасности, в 2012 году 80% атак было реализовано с благонадежных сайтов, зараженных вредоносным кодом, при этом почти 18% доменов с эксплойтами Blackhole находились в России.

В прошлом году пароли пользователей LinkedIn оказались опубликованными благодаря российским хакерам – в архиве было 6,5 млн паролей. То же коснулось и Formspring, 420 тысяч паролей появились в Интернете. Полмиллиона паролей потерял Yahoo Voices. Базу данных компании Philips дважды ломали хакеры. Было опубликовано более 200 тыс. писем электронной почты, 1 тыс. из которых содержит важные учетные данные. Крупнейший интернет-магазин Zappos был взломан: злоумышленники украли у компании данные 24 миллионов клиентов (имена, адреса электронной почты, номера мобильных телефонов и последние четыре цифры кредитных карт).

Объединив информацию из открытых источников и мнения IT-экспертов, можно составить рейтинг наиболее распространенных кибератак:

1. Троянские вирусы

Использующие социальную инженерию троянские вирусы являются первым способом атаки. Конечный пользователь просматривает веб-сайт, запуская тем самым троянский вирус. В большинстве случаев веб-сайт является законным, но подвергся хакерской атаке.

Обычно на странице веб-сайта появляется сообщение о том, что пользователь подвергся вирусной атаке и должен запустить поддельное антивирусное программное обеспечение. А также сообщение о том, что у пользователя практически закончилось свободное место на диске и ему необходима дефрагментация. Пользователь запускает программу, пропуская предупреждение браузера о том, что программа может быть вредоносной. Использующие социальную инженерию троянские вирусы вызывают сотни миллионов действенных хакерских атак каждый код. В сравнении с этими цифрами все

другие типы хакерских атак – просто пустой звук.

2. Неисправленное программное обеспечение

Второе место занимает программное обеспечение с известным, но неисправленным вредоносным кодом. Наиболее распространенными неисправленными и используемыми программами являются Java, Adobe Reader и Adobe Flash. Так происходит уже на протяжении нескольких лет. К сожалению, исправить полностью эти программы компаниям-производителям пока не удается.

3.Фишинговые атаки

В отличие от предыдущих «грубых» взломов фишинговые атаки, как считают специалисты, – противозаконное произведение искусства. В нем не сразу разглядишь подделку, все выглядит безупречно: содержится предупреждение о том, чтобы пользователь проявлял осторожность в отношении мошеннических электронных сообщений. И потому для борьбы с ним требуются специальные антифишинговые инструменты.

4. Гуляющие в Сети «черви»

Компьютерные вирусы больше не представляют угрозу, в отличие от их братьев – гуляющих в Сети «червей». Большинству организаций пришлось бороться с такими «червями», как Conflicker и Zeus. Мы не наблюдаем масштабных вспышек, которые имели место в прошлом, с «червями», содержавшимися в приложениях к сообщениям электронной почты, однако их разновидность – гуляющие в Сети черви – могут укрываться гораздо лучше, чем их родственники, находившиеся в сообщениях электронной почты.

5. Целенаправленные устойчивые угрозы (ЦУУ), или Advanced Persistent Threat

ЦУУ осуществляют с целью похищения интеллектуальной собственности. ЦУУ обычно опираются на использующие социальную инженерию троянские вирусы или фишинговые атаки. Запускается фишинговое электронное сообщение с троянским вирусом, на которое обязательно отреагирует кто-нибудь из сотрудников фирмы. После первого «захвата» компьютера злоумышленники могут всего за несколько часов взломать все компьютеры предприятия. Противостоять угрозам может только четко выстроенная система защиты.

Аналитическая компания в области исследований защиты от любого рода вредоносного трафика Imperva в 2012 году обозначила еще две новых разновидности кибератак, которые называются business logic attacks (BLA-атаки) – это коммент-спам и извлечение e-mail адреса, наиболее «популярные» в Восточной Европе.

Кибер-рискам особенно подвержены крупные компании, поскольку они создают информационные системы, состоящие из большого количества компонентов, в которых содержатся обширные базы данных. Это могут быть и условия договоров, и деловая переписка, и пароли от личных кабинетов.

В сложившейся ситуации успех страхового продукта CyberEdge от компании AIG вполне закономерен. При наступлении страхового случая компания получает консолидированную поддержку в сфере IT, антикризисных коммуникаций и юридических вопросов, связанных с последствиями инцидента. Также предусмотрена компенсация убытков, возникших в результате нарушения безопасности данных страхователем или его субподрядчиком, включая убытки, возникшие по причине нарушения безопасности компьютерной сети. Могут быть возмещены расходы на реагирование, включая расходы на техническую экспертизу, восстановление репутации страхователя и должностных лиц страхователя, мониторинг возможных злоупотреблений данными и восстановление электронных данных. Также компенсируются сборы, расходы и издержки на юридические консультации и представительство в связи с расследованием, проводимым государственными органами.

Деятельность любой компании сейчас поставлена в зависимость от интернет-ресурсов в полном смысле слова. Стоит задуматься, насколько компания подготовлена к неприятному сюрпризу в виде пропажи базы данных клиентов? А к раскрытию личной переписки в социальных сетях? С каждым годом взломщики становятся все изощреннее: хакеры способны взломать сложные пароли, скопировать конфиденциальную информацию, уничтожить вашу информационную базу и так далее. Очевидно, не стоит откладывать на завтра то, что может обезопасить вас уже сегодня.

Источник: www.wiki-ins.ru, 16.01.13

Автор: Ланская А.