Необходимость компьютерной безопасности в корпоративной сети

Бабушкин Никита Сергеевич,
магистр МИРЭА,
Россия, Москва

На данный момент вопрос о компьютерной безопасности встает намного чаще чем ранее. Данная тема более важна и необходимо к рассмотрению чем может показаться на первый взгляд. Она касается не только крупных владельцев бизнесов, использующие повсеместно громоздкие системы из нескольких десятков компьютеров и иных технических средств, хранящих на своих носителях коммерческие тайны. Но и так же пользователей персональных компьютеров , личных технических устройств, временами обращающийся в всемирную сеть.

Компьютерная сеть полностью защищена лишь тогда, когда она полностью автономна и отключена . Какое либо отклонение от данного состояния подвергает техническое устройство к потенциальным угрозам.

Каким же образом проявляются эти угрозы? В общих чертах — это вероятность правонарушителя каким либо образом воспользоваться ресурсами компьютера или иного технического устройства, подвергнуть изменению информации, украсть интересующие его данные и использовать в своих личных целях. К примеру даже если оплата никогда не производилась с помощью данного компьютера и банковский счет не как не привязан к нему, электронные письма с содержанием которое должно сохраняться в секрете, информация о том какие сайты, в какой промежуток времени и какая деятельность там ввелась, может навредить.

За последние три десятилетия информационные технологии просочились все слои координирования и ведения бизнеса. Так и само существование бизнеса плавно переходит из физического мира в виртуальный, из-за этого является мишенью, для хакерских атак злоумышленников. По данным Института Компьютерной Безопасности общий ущерб, нанесенный компьютерными вирусами за последние 5 лет, оценивается примерно в 155 млрд. долларов.

Министерство национальной безопасности Соединенных Штатов Америки, сравнило вирусные эпидемии к терроризму. Современные разработчики программного оборудования, стараются как можно быстрее реагировать на атаки, но после , а не заранее. На данный момент времени не изобретено способов защиты от глобальных эпидемий вирусов.

Одни из первых преступлений с участием компьютерной техники появились в России в 1991г., когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР. В2014 г. МВД зарегистрировало в России 11 000 компьютерных преступлений, на долю краж и мошенничеств в 2014 г. пришелся 41% киберпреступлений (в 2013 г. этот показатель составлял 30%).

Эксперты утверждают, что вести подсчет киберпреступлений крайне затруднительно, но общее их количество изрядно превышает данные из статистики МВД. Реальное картина киберпреступлений в России, минимум в 5 раз больше, как подсчитывает компания Digital Security.

С 1999 года так же появилась очередная проблема для информационной безопасности — СПАМ. Это повсеместная анонимная не желаемая рассылка . На данный момент спам достиг около 1/3 всех электронных сообщений. Избыток спама ведет к ежегодным убыткам, которые по оценке экспертво насчитывают до 20 млн. долларов США. Не желательная рассылка в границах одной организации , ведет к потерям от 500 до 1000 долларов США ежегодно в расчете

на 1 пользователя.

«Спам — это архиважная проблема, грозящая свести на нет большую часть преимуществ электронной почты», — пишет Билл Гейтс в одном из своих регулярных e-mail-обращений к заказчикам.

В свою очередь широко распространяется и промышленный шпионаж — не большое устройство стоимостью всего 10 долларов США, в случае грамотного расположения, может привести крупную организацию к разорению.

На данный момент времени злоумышленники могут заполучить доступ не только к открытой информации , но и к информации охватывающей государственную и коммерческую тайны.

В заключении можно сделать вывод, что на сегодняшней день, компании должны иметь стратегию информационной безопасности, основывающейся на комплексном подходе защиты информации, осуществлять аудит всех компонентов информационной безопасности и иметь подготовку к будущему.