УДК 004.491 004.492 004.493 004.514.6 004.77

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Пасько Д.П.

Научный руководитель – к.т.н., доцент Сизиков С.В.

Для человеческой глупости нет предела (Кевин Митник).

Именно с этого высказывания я бы хотел начать свою статью. В настоящее время вопрос информационной безопасности становится все острее. Для начала предлагаю разобраться с термином информационная безопасность.

Информационная безопасность (англ. Information Security, а также — англ. InfoSec) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

В моем выступлении речь пойдет о наиболее актуальном и обширном разделе информационной безопасности – компьютерной безопасности. Также будет подыматься вопрос безопасности персональных данных в целом и прочие.

Интернет представляет собой наибольшую угрозу безопасности. Поэтому первый вопрос, который я хочу поднять это анонимность в интернете.

Когда вы говорите, что вам нечего скрывать, вы, по сути, заявляете, что вам плевать на свои права. © (Эдвард Сноуден).

Список необходимых, по мнению Сноудена, действий для повышения своей анонимности, а, следовательно, и безопасности, в сети:

- шифрование голосовых вызовов и текстовых сообщений;
- шифрование жёсткого диска;
- использование менеджеров паролей;
- применение двухакторной аутентификации;
- использование TOR.

Важно понимать, что ваши персональные данные (будь то номер банковской карты или просто ваше настоящее имя), в лучшем случае, не должны появляться в сети вообще. Потому что абсолютно любая информация, что на ваш взгляд не имеет никакого веса, на самом деле может быть использована злоумышленником. Например, оставленные на вашей странице, в социальной сети имени, фамилии и номера телефона будет достаточно для регистрации на каком-либо сайте. Вы можете сказать, что данный, пример, не так страшен, однако не стоит забывать, что ваши персональные данные в таком случае уже были скомпрометированы. Однако если, используя фотографию вашего лица на фоне паспорта (которое может быть получено мошенниками, например, из базы данных букмекерской конторы), на ваше имя будет оформлен условный кредит, то идея регистрации, на похожих сайтах, уже не покажется вам такой безобидной.

Но, большинство людей, попросту не захочет пользоваться тоннами анонимайзеров для того, чтобы найти в интернете смешную картинку с котами.

Однако это не отменяет всего вышесказанного, поэтому важно знать и использовать какие-то основные правила аккуратного поведения в интернете:

1. Не регистрируйтесь на сайтах, которым не доверяете
2. Не сообщайте ни под каким предлогом свои персональные данные кому-либо в интернете
3. Будьте внимательны при переходе по ссылкам, иногда, может быть, достаточно просто посмотреть, на путь, по которому она ведет
4. Помните, что в интернете не все желают вам добра, там много мошенников

И это лишь “вершина айсберга” безопасности в интернете.

А теперь представим, что злоумышленник не хочет с вами “общаться” и решил заполучить ваши данные с помощью коварной программы – вируса.

Компьютерный вирус – вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Так как же нам защитить себя от вредоносных программ?

Во-первых, самое главное, что стоит делать при работе не только с устройством, но работе в интернете – это быть внимательным. Да, именно невнимательность пользователя приводит к утечке его персональных данных.

Во-вторых, снова быть внимательным, потому что большинство не понимает смысла этого слова.

И в-третьих, использовать программы-антивирусы, и что немаловажно, следить и регулярно обновлять их до последней версии, потому что с выходом каждого обновления база данных “антивируса” пополняется новыми видами вирусов и их разновидностями, а, следовательно, повышается вероятность, что в случае попадания вируса на ваше устройство, антивирусная программа успешно обнаружит и ликвидирует его.

Но что делать, если вы все-таки заполучили необходимый вам файл и хотите быть уверены, что он не скрывает в себе, какого-то, вредоносного ПО? Во-первых, замечательно, что вы уже задумались над этим, вместо того, чтобы бездумно открыть ваш файл. А во-вторых, можно, к примеру, воспользоваться онлайн-сканером вирусов (таким как virus total).

А чтобы, опять-таки, не делать лишних телодвижений для получения информации в интернете, можно обезопасить себя заранее, просто пользуясь официальными источниками. К примеру, если вы хотите установить пакет Microsoft Office, то вам следует перейти на сайт microsoft.com и скачать и установить лицензионное ПО. Да, вам будет необходимо оплатить продукт, но если мы говорим о безопасности, то это будет лучшим решением.

Кроме того, очень важно знать, что обновление ОС – это тоже необходимость. Не все злоумышленники пользуются каким-либо вредоносным ПО, некоторые предпочитают эксплуатировать дыры в безопасности самой системы. Например, нашумевший с недавних пор, в связи с расследованием Сноудена, эксплоит EternalBlue использует уязвимость CVE-2017-0144 в SMB-протоколе Windows, что естественно не осталось незамеченным

разработчиками из Microsoft и уже через месяц они выпустили патч, который залатал эту дыру. Так вот, если вы не обновляли систему уже некоторое время, то вполне вероятно, что данную уязвимость можно обнаружить и на вашем компьютере.

Кстати говоря, злоумышленнику могут быть без надобности ваши персональные данные, следовательно, после заражения компьютера вы можете даже не заметить наличия чего-то постороннего. Так зачем же тогда заражать ваш компьютер, ради удовольствия что ли? Конечно же нет. Злоумышленнику может быть полезна вычислительная способность вашего компьютера, возможно именно ваша машина является частью ботнета.

Ботнет (botnet) – сеть компьютеров, которая состоит из некоторого количества хостов, с запущенными ботами – программами, которые устанавливаются на компьютер жертвы без ее ведома и дают злоумышленнику возможность выполнять некие действия с использованием ресурсов зараженного компьютера.

И если вам кажется, что это не принесет вам никакого дискомфорта, то спешу вас огорчить: кроме банально медленной работы компьютера вы можете стать частью крупной ddos атаки на какой-нибудь сервер, а это уже уголовно наказуемо.

Итак, мы переходим к теме, которую не затрагивали до сих пор, а именно безопасность сетей WiFi. Да, возможно вы поддерживаете версии своего ПО и системы, в общем, в актуальном на данный момент состоянии, возможно, ваш компьютер настолько хороший оплот, что его не берет ни один вирус на планете, но, тем не менее, ваши данные все равно могут быть скомпрометированы. Так как же это происходит? А все очень просто, дело, опять-таки, в невнимательности пользователя, и сейчас я говорю про пользователя какой-либо точки доступа WiFi. В наше время это представляет довольно серьезную угрозу безопасности, поскольку “открытых” точек огромное количество и не каждый человек, подключаясь к одной из них, подозревает, что его данные могут быть похищены таким способом.

Поэтому, прежде всего, стоит запомнить: не пользуйтесь общественными сетями. Да, именно так, ведь сейчас мы говорим об абсолютной безопасности.

А также нужно затронуть еще один момент, который кстати я неумышленно не поднимал выше – надежность пароля. Это касается как владельца точки доступа, так и любого клиента всемирной паутины. Поэтому важно, всегда и везде, использовать надежные пароли, и говоря надежные, я имею в виду, не один для всего, что только можно. Пароли типа AnnaTheBest или GoodBoy, как вы уже поняли, не являются надежными. Кстати в интернете есть огромное количество ресурсов, которые предлагают проверить не только стойкость вашего пароля, но и его наличия в словарях для брута или какой-то слитой в сеть базы данных.

Давайте разберемся, из чего должен быть собран ваш пароль, чтобы злоумышленник не смог его подобрать:

- набор цифр;
- набор букв;

- набор спецсимволов;
- вариация регистра;
- длинный;
- смысл, очевидный только вам.

Например, такой пароль будет более-менее надежным: MasterQaZ-12@H9.

И чего в нем быть не должно:

- имена (ваше, вашей мамы, сестры, домашнего питомца и т.п.);
- последовательность цифр или/и букв (qwerty, 12345678, qwerty12345 и т.п.);
- слишком короткий;
- номер телефона.

Вот такой пароль использовать не стоит: Anton228.

Все вышесказанное, без сомнения, показывает важность информационной безопасности, особенно сегодня. В настоящее время, когда практически невозможно найти семью, в которой не будет ни одного гаджета, обучение информационной безопасности становится в одну строку важности с правилами дорожного движения.

Тема компьютерной безопасности не поднимается в кругах рядовых пользователей, не имеющих отношения к смежным специальностям. Как результат этого – наличие на многих компьютерах вирусных программ.

Для того, чтобы избежать подобных массовых заражений, необходимо проводить обширную образовательную политику. Все категории пользователей должны быть осведомлены об устройстве информационной безопасности.

Большое количество уверенных пользователей компьютера считают, что их не коснется проблема информационной безопасности. Однако это не так, ведь без специальных знаний невозможно полностью оградить себя от опасности.

Для получения этих специальных знаний необходимо внедрять смежные дисциплины в учебную программу, ведь информационная безопасность касается детей ничуть не в меньшей степени, чем взрослых. Что же касается категории пользователей, которые уже не обучаются ни в одном образовательном заведении, необходимо организовывать тематические лекции и семинары, ведь если речь идет о сотрудниках большого офиса, то незнание азов информационной безопасности может повлечь последствия не только для конкретного пользователя, но и для всей организации в целом.

И помните: сама большая дыра в интернете сидит перед вашим монитором. ©

Литература

1. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. “Атака на интернет”
2. Издательского дома "Открытые Системы" (Lan Magazine/Журнал сетевых решений, 1996, том 2, #7)
3. Издательского дома "Открытые Системы"(Сети, 1997, #8)
4. “Office” N5 1999 Александр Буров “Человеческий фактор и безопасность”