ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.9

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ВЫЗОВЫ СОВРЕМЕННОГО МИРА

© 2017 Ю. П. Преображенский

Воронежский институт высоких технологий

Аналитический обзор посвящен актуальным аспектам обеспечения компьютерной безопасности как для обычных пользователей, так и для корпоративного сегмента. Обзор предназначен для аспирантов или магистров, выбирающих направление для своих научно-практических исследований в сфере информационной безопасности.

Ключевые слова: информационная безопасность, защита информации, компьютерные системы.

Едва ли найдется современный человек, который бы не пользовался достаточно продвинутыми устройствами-гаджетами – мобильным телефоном или планшетом, которые обладают высокоскоростным доступом в интернет, камерой высокого разрешения и немалой вычислительной мощностью. Обычно такие устройства имеют настройки по умолчанию, например, позволяющие отправлять фотографии непосредственно в облачное хранилище, что позволяет показать их друзьям и коллегам в любом месте и в любое время. Хранить документы на USB-носителе тоже становится немодным, облака вытесняют привычную процедуру «сбросить на флешку». Одновременно с этим владельцы документов, фотографий и гаджетов обычно даже не задумываются о том, отвечает ли администрация облачного сервиса за конфиденциальность и сохранность его фотографий и документов. Именно непонимание степени риска столь обширного доверия публичным облачным технологиям приводит к регулярному появлению на просторах сети документов или даже интимных фотографий и весьма неприятным сюрпризам для их владельцев.

Рядом с описанной выше ситуацией стоит технология BYOD – Bring Your Own Device, позволяющая корпоративным работникам использовать свои собственные ноутбуки, планшеты или телефоны для работы в информационной инфраструктуре компании.

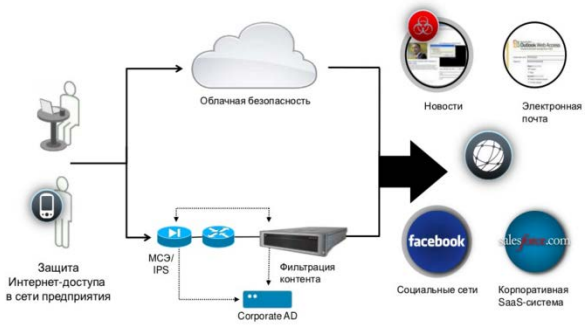

Рис. 1. Технология BYOD требует выработки стратегии защиты

Достаточно небрежное отношение к таким устройствам со стороны их владельцев может привести к утечке чувствительных корпоративных секретов просто при утере мобильного телефона или при внешне ничего не значащей передаче на некоторое время BYOD-планшета родственникам.

Все мы любим привозить из отпуска или командировки сотни фотографий, однако, мало кто задумывается о том, чтобы сделать резервную копию этих цифровых впечатлений. Задуматься об этом человеку приходится ровно через секунду после того, как он обнаруживает, что раздел жесткого диска с фотографиями не открывается, или в момент падения внешнего жесткого диска с полки шкафа на пол. Реанимировать утраченные фотографии или даже целые цифровые семейные архивы иногда можно, однако

Преображенский Юрий Петрович – ВИВТ АНОО ВО, начальник отдела информатизации и менеджмента качества, к.т.н., профессор, it_pro@vivt.ru.

этой ситуации вообще можно было бы избежать, задумайся их владелец о резервировании вовремя, а не пост-фактум. Аргумент «второй жесткий диск для резервных копий – это дорого» обычно не приводится в ответ на вопрос: «А сколько вы готовы заплатить за восстановление своих документов или фотографий?»

Рис. 2. Схема взаимодействия и управления облачным хранилищем

С экрана телевизора и в многочисленных Интернет-статьях в настоящее время активно рассказывается о мощном движении вперёд биометрических средств аутентификации, в частности об использовании отпечатков пальцев для подтверждения платежей или просто разблокировки гаджета. Задумываемся ли мы, что в случае компрометации нашего пароля (его случайно подсмотрел посторонний) или его банальном забывании, мы без особых проблем можем поменять пароль. Можем ли мы поменять отпечатки пальцев, которые мы оставляем практически везде? Можно ли похитить у человека его отпечатки пальцев так, чтобы он не знал об этом? К сожалению, это не такая уж сложная техническая задача.

Следующая проблема современного мира информационных технологий – суровая привязанность к постоянному наличию Интернет-подключения. В торговом центре, кафе, гостинице или даже в поезде многие инстинктивно начинают проверять доступность открытой WiFi-сети, особо не задумываясь о степени её надежности и безопасности. Это может быть поддельная беспроводная сеть с красивым логичным именем, например, совпадающим с названием кафе или гостиницы, к которой радостно подключатся посетители, оставляя свою конфиденциальный трафик совершенно постороннему человеку. Обязательно ли злоумышленник ей воспользуется? Неизвестно. Но вероятность утраты доступа к своей учетной записи социальной сети или иных аналогичных проблем весьма и весьма велика.

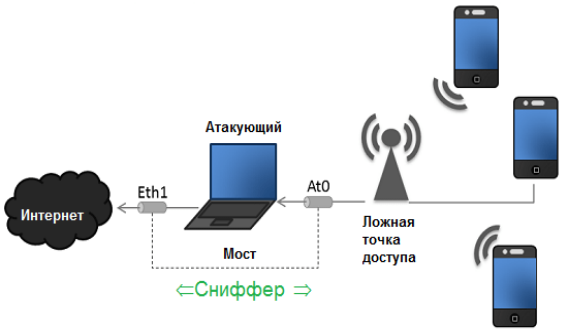

Рис. 3. Схема применения ложной точки беспроводного доступа

Симпатичные квадратики из точек, так называемые QR-коды, очень популярны к размещению на арт-объектах, памятниках архитектуры, да и даже на обычных продуктах, вот только однозначную гарантию того, что, например, размещенный QR-код на плакате в аэропорту является валидным, дать, к сожалению, невозможно. Для злоумышленника наклеить поддельный QR-код поверх настоящего – дело доли секунды, тогда как потенциальный ущерб от использования такого кода ни о чем не подозревающими путешественниками просто огромен.

Говоря о более простых вещах, нежели QR-коды или гаджеты с камерой, следует сказать о паролях. «Не спрашивать больше», «Запомнить пароль» – эти отметки крайне любимы пользователями, которые забывают простую истину: «Удобно? Значит потенциально небезопасно!»

Безусловно, входить в почтовый ящик или учетную запись социальной сети одним щелчком мыши крайне удобно, однако, в случае утери гаджета, это с такой же лёгкостью сможет сделать и посторонний человек. Маловероятно, что сразу после того, как пользователь не найдет в своём кармане мобильный телефон, он бросится искать Интернет-подключение для смены паролей. Не говоря уже о том, что в случае подключения к номеру мобильного телефона услуги «Мобильный банк», утрата гаджета обернется еще и существенными финансовыми потерями.

Пароли, которые используют пользователи, очень часто социализированы: имена, фамилии, даты рождения, прозвища, любимые словечки, стоящие рядом на клавиатуре комбинации букв и цифр – всё это пользователи очень любят использовать в качестве паролей. Меняют ли неискушённые в вопросах информационной безопасности пользо-

ватели пароли с некоторой периодичностью? Увы, нет. Заставить пользователя сменить пароль, который используется уже неприлично долго, может движок форума или социальной сети, однако и здесь пользователь будет стремиться обмануть систему так, чтобы по возможности оставить старый пароль, дабы не запоминать новый.

Допустим, мы объяснили пользователю риски социализации паролей и тот факт, что пароль «Lena123» недостаточно хорош. Следует спросить, а сколько паролей к различным ресурсам вообще есть у пользователя? Наиболее частый ответ – не больше двух. С развитием Интернет-технологий пользователи вообще сводят процедуру авторизации к щелчку по иконке социальной сети, очередной раз эксплуатируя принцип «Это удобно». Задумывается ли пользователь, сколько ресурсов можно использовать, завладев его учетной записью? Увы, нет.

Вряд ли найдется хоть один пользователь Интернет, который бы не столкнулся с попыткой фишинга (fishing), то есть с поддельными сайтами, внешне выглядящими как настоящие и собирающими учетные данные пользователей. Пользователь может и не обратить внимания на лишнюю или неправильную букву в адресе сайта, или на подозрительно длинный URL ресурса (sberbanc.ru, tvitter.com или аналогичное), собственноручно вписав в поля «Имя пользователя» и «Пароль» свои данные. Индустрия фишинга – одна из самых мощных, здесь требуются усилия и веб-дизайнеров, и программистов, никто не чурается никаких методов, главное – выманить у пользователя пароль к ресурсу-двойнику.

Говоря о степени безопасности персональных данных, нельзя не отметить тотальное пренебрежение пользователями самыми простыми и очевидными вещами, например, не стоит вводить сведения о себе в различные поисковые формы «Баз данных всех граждан России», которые, например, открываются по ссылкам из писем, проскочивших спам-фильтры. Весьма сложно объяснить пользователю или простому обывателю, почему делать подобное на портале государственных и муниципальных услуг можно с определенной степенью уверенности, а на сайте vsepersonyrf.com – нет. Любопытство, с которым начинающий пользователь Всемирной паутины пытается узнать, что есть в Сети о нём, оборачивается для него весьма дорого.

Любая корпоративная информационная инфраструктура состоит из двух компонентов – люди и оборудование. Как известно, любой аппаратный компонент может выйти из строя, любая программа может однажды засбоить, но всё равно самое слабое звено в любой системе – человек. Психология сотрудников любой компании – потенциальная мишень для злоумышленника, владеющего навыками и методиками социальной инженерии. Практически все они основаны на речевом или аудиовизуальном воздействии на жертву: телефонный звонок, письмо по электронной почте, либо подложные изображения с одновременным разговором по Skype и т. п.

Большая часть атак на базе социальной инженерии происходит по телефону или посредством электронной почты. Маловероятен приход злоумышленника в офис лично, тогда как отправить электронное письмо или позвонить начинающему специалисту с предложением, просьбой или вопросом – элементарно и ничего не стоит злоумышленнику. Либо жертву обманом вынуждают продиктовать закрытую информацию (например, логин/пароль или закрытый IP-адрес для корпоративной сети), либо выполнить некоторые действия, если злоумышленник выдает себя за ИТ-сотрудника той же компании. Поскольку социальной инженерии подвластны и молодые, и крайне опытные сотрудники (вопрос только в подходе и степени заинтересованности злоумышленника), необходимы постоянные тренировки и внутренний аудит безопасности с достаточно жесткими последствиями для нарушителей [1, 2].

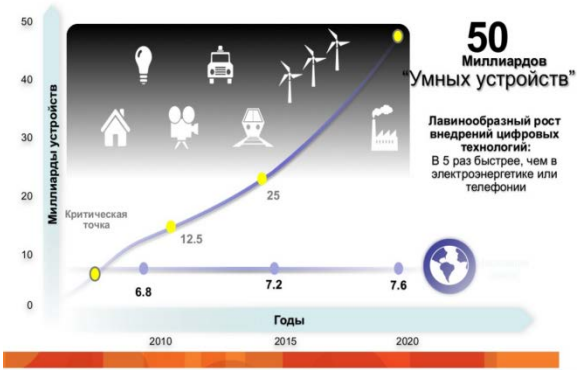

Рис. 4. Прогнозы развития Интернета вещей

И еще несколько слов о вызовах безопасности завтрашнего дня. Одной из технологий, за которой, без всякого сомнения, будущее, является Интернет вещей (Internet of

Things или Internet of Everything). Холодильники, автоматически следящие за сроком годности продуктов в них, «умные» цветочные горшки, напоминающие о необходимости полива и информирующие о росте кактусов своих владельцев – сейчас это вызывает улыбку, однако завтра мы будем покупать все эти устройства в наших магазинах.

В настоящее время идут бурные многочисленные обсуждения – насколько безопасен будет мир таких умных вещей? Не будет ли микроволновая печь следящим за хозяином инструментом злоумышленника? Не позволит ли недостаточно безопасный умный цветочный горшок хакеру проникнуть в домашнюю сеть? Сегодня ответов на эти и подобные вопросы в общем нет. Проникновение в нашу жизнь беспроводных и Интернет-технологий лишь ускоряет развитие принципов информационной безопасности, выполнять требования которых необходимо всем нам, живущим в 21 веке.

ЛИТЕРАТУРА

1. Львович И. Я. Факторы угрозы экономической безопасности государства // И. Я. Львович, А. А. Воронов, Ю. П. Преображенский / Информация и безопасность. 2006. – Т. 9. – № 1. – С. 36-39.

2. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности // А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов / Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

INFORMATION SECURITY - THE CHALLENGES OF THE MODERN WORLD

© 2017 Yu. P. Preobrazhenskiy

Voronezh Institute of High Technologies

The review is devoted to the topical aspects of computer security for both ordinary users and for the corporate segment. The review is intended for graduate students or masters who choose the direction for their scientific and practical research in the field of information security.

Keywords: information security, information protection, computer system.