18+

Владимир Безмалый

Цифровая гигиена

Том I

Владимир Безмалый

Цифровая гигиена. Том I

«Издательские решения»

Безмалый В.

Цифровая гигиена. Том I / В. Безмалый — «Издательские решения»,

ISBN 978-5-44-852165-2

У вас в руках универсальный учебник, который совсем не похож на учебник. Читайте сначала и до конца или с любого случайно открытого места. Читайте сами, своим детям перед сном или своему боссу по пути в аэропорт — всё будет не зря. Герои книги — принцессы и драконы, шпионы и контрразведчики, не оставят читателей равнодушными и оставят в памяти читателя и слушателя сценарии правильного поведения в кибер-среде и способы лёгкого и изящного обхода угроз.

ISBN 978-5-44-852165-2

Содержание

Цифровая гигиена
Том I
Владимир Безмалый

ISBN 978-5-4485-2165-2
Создано в интеллектуальной издательской системе Ridero

Введение

В нынешнем гипер-информатизированном мире роль специалистов по информационной безопасности сегодня такая же, какая была сто лет назад у врачей. Кто-то создаёт вакцины от смертельных болезней, кто-то изучает и классифицирует виды бактерий, кто-то спасает уже заболевших, а кто-то учит ещё здоровых, как вести себя, чтобы не заболеть: например, мыть руки перед едой и не пить воду из луж,

Книга, которую вы держите в руках – лучший из известных мне образцов пособий по «цифровой гигиене». Без наукообразных терминов в виде коротких поучительных историй автор рассказывает очень важные для информационной безопасности личности и предприятия вещи, иногда прямо, а иногда исподволь внушает нам, как сохранить свою приватность в этом новом и непривычно открытом кибер-мире. Как защитить себя от мошенников и «похитителей личностей». Как безопасно и одновременно очень удобно проводить платежи, не выходя из дома и многое, многое другое.

Мир станет честней и безопасней, когда «цифровая гигиена», то есть набор правил безопасного поведения в цифровом пространстве, войдёт в ежедневную рутину каждого пользователя информационных технологий. Можно было сколько угодно выпускать учёных-эпидемиологов, врачей и гигиенистов, но пока каждый человек на планете не научился мыть руки, человечество не смогло бы победить страшные болезни. То же самое должно произойти и в кибер-пространстве, тогда «врачам» останется только двигать науку вперёд, а не бесконечно бороться с эпидемиями.

У вас в руках универсальный учебник, который совсем не похож на учебник. Читайте сначала и до конца или с любого случайно открытого места. Читайте сами, своим детям перед сном или своему боссу по пути в аэропорт – всё будет не зря. Герои книги – принцессы и драконы, шпионы и контрразведчики, не оставят читателей равнодушными и оставят в памяти читателя и слушателя сценарии правильного поведения в кибер-среде и способы лёгкого и изящного обхода угроз. Надеюсь, автор выпустит книгу и в аудио-формате и я смогу слушать её ещё и в перелётах.

Наслаждайтесь. Оно того стоит.

Рустэм Хайретдинов, друг и поклонник автора.

Али-Баба и сорок разбойников

Старая сказка с новыми знаниями. Мудрость вековая, а знания по ИБ сегодняшние

Когда-то, очень давно, в одном персидском городе жили два брата – Касим и Али-Баба. Когда умер их отец, они поделили деньги, которые после него остались, и Касим стал торговать на рынке дорогими тканями и шелковыми халатами. Он умел расхваливать свой товар и зазывать покупателей, и в его лавке всегда толпилось много народу. Касим все больше и больше богател и, когда накопил много денег, женился на дочери главного судьи, которую звали Фатима.

А Али-Баба не умел торговать и наживать деньги, и женат он был на бедной девушке по имени Зейнаб. Они быстро истратили почти все, что у них было, и однажды Зейнаб сказала:

– Слушай, Али-Баба, нам скоро будет нечего есть. Надо тебе что-нибудь придумать, а то мы умрем с голоду.

Читателю Сидя на диване, денег не заработаешь! *. Запомни, дорогой друг, рано или поздно халява всегда заканчивается и приходится вставать с дивана и что-то делать. Это же можно сформулировать как первое сказочное правило ИБ.*

– Хорошо, – ответил Али-Баба, – я подумаю, что нам делать.

Он вышел в сад, сел под дерево и стал думать. Долго думал Али-Баба и наконец придумал. Он взял оставшиеся у него деньги, пошел на рынок и купил двух ослов, топор и веревку.

А на следующее утро он отправился за город, на высокую гору, поросшую густым лесом, и целый день рубил дрова. Вечером Али-Баба связал дрова в вязанки, нагрузил ими своих ослов и вернулся в город. Он продал дрова на рынке и купил хлеба, мяса и зелени.

С тех пор Али-Баба каждое утро уезжал на гору и до самого вечера рубил дрова, а потом продавал их на рынке и покупал хлеб и мясо для себя и для Зейнаб.

Читателю *. Запомни дорогой друг, если все что ты умеешь, это просто тупо рубить дрова (нажимать на кнопки), то делать это можно бесконечно. Правда хватать тебе будет только на хлеб. Иногда с маслом и мясом. А чтобы заработать – нужно думать и учиться. Или учиться и думать.*

И вот однажды он стоял под высоким деревом, собираясь его срубить, и вдруг заметил, что на дороге поднялась пыль до самого неба. А когда пыль рассеялась, Али-Баба увидал, что прямо на него мчится отряд всадников, одетых в панцири и кольчуги; к седлам были привязаны копья, а на поясах сверкали длинные острые мечи. Впереди скакал на высокой белой лошади одноглазый человек с черной бородой.

Али-Баба очень испугался. Он быстро влез на вершину дерева и спрятался в его ветвях. (А всадники подъехали к тому месту, где он только что стоял, и сошли на землю. Каждый из них снял с седла тяжелый мешок и взвалил его себе на плечи; потом они стали в ряд, ожидая, что прикажет одноглазый – их атаман. ***Читателю.*** *Вовремя спрятаться не трусость, а просто тактика выживания. Но запомни, спрятавшись, на хлеб с маслом не заработаешь.)*

«Что это за люди и что у них в мешках? – подумал Али-Баба. – Наверное, это воры и разбойники».

Он пересчитал людей, и оказалось, что их ровно сорок человек, кроме атамана. Атаман встал впереди своих людей и повел их к высокой скале, в которой была маленькая дверь из стали; она так заросла травой и колючками, что ее почти не было видно.

Читателю. *Какую ошибку совершил атаман? Он забыл о том, что в пути (в любой работе) нужна разведка (предварительное исследование пути к объекту и продумывание возможных последствий и путей отхода). Кто тупо идет вперед не смотря по сторонам, рано или поздно попадает в лужу.*

Атаман остановился перед дверью и громко крикнул:

– Сим-сим, открой дверь!

И вдруг дверь в скале распахнулась, атаман вошел, а за ним вошли его люди, и дверь опять захлопнулась за ними.

Читателю. *В чем ошибка атамана? Он передает пароль по открытому беспроводному каналу. Голосом! Громко! А что нужно? Если вы используете беспроводной канал связи – используйте шифрованный канал. Если это невозможно – занизьте уровень сигнала (в данном случае голоса) до минимально необходимого. Используйте аутентификацию с помощью OneTimePassword. Проводите этот сеанс на минимальном расстоянии до вашего роутера (в данном случае двери), чтобы снизить возможность перехвата. Современный пример – применяйте беспроводную сигнализацию с перешифрованием (OneTimePassword) и на минимальном расстоянии от вашего автомобиля.*

«Вот чудо! – подумал Али-Баба. – Ведь сим-сим-то – это маленькое растение. Я знаю, что из него выжимают масло, но я не знал, что оно может открывать двери!»

Али-Бабе очень хотелось посмотреть поближе на волшебную дверь, но он так боялся разбойников, что не осмелился слезть с дерева.

Читателю. Лучше быть параноиком, но ЖИВЫМ! *На самом деле иногда важно перестраховаться.*

Прошло немного времени, и вдруг дверь снова распахнулась, и сорок разбойников вышли с пустыми мешками. Как и прежде, одноглазый атаман шел впереди. Разбойники привязали к седлам пустые мешки, вскочили на коней и ускакали.

Тогда Али-Баба, который уже устал сидеть скорчившись на дереве, быстро спустился на землю и подбежал к скале.

«А что будет, если я тоже скажу: „Сим-сим, открой дверь?“ – подумал он. – Откроется дверь или нет? Попробую!»

Он набрался храбрости, вдохнул побольше воздуху и во весь голос крикнул:

– Сим-сим, открой дверь!

Читателю. *И снова та же ошибка. Ну зачем же орать? А вдруг атаман кого-то оставил? А в чем ошибка атамана? Важный объект (в данном случае дверь) всегда должны быть с включенной сигнализацией и видеоконтролем. Так дверь в серверную всегда должна быть закрыта, видеоконтроль должен срабатывать при каждом открывании двери, охрана должна вести журнал, в котором контролировать вход-выход.*

И тотчас же дверь распахнулась перед ним, и открылся вход в большую пещеру.

Али-Баба вошел в пещеру, и, как только он переступил порог, дверь снова захлопнулась за ним. Али-Бабе стало немного страшно: а вдруг дверь больше не откроется и ему нельзя будет выйти? Но он все же пошел вперед, с удивлением осматриваясь по сторонам.

Он увидел, что находится в большой комнате и у стен стоит множество столиков, уставленных золотыми блюдами под серебряными крышками. Али-Баба почувствовал вкусный запах кушаний и вспомнил, что с утра ничего не ел.

Он подошел к одному столику, снял крышки с блюд, и у него потекли слюнки, – на блюдах лежали все кушанья, каких только можно пожелать: жареные куры, рисовый пилав, блинчики с вареньем, халва, яблоки и еще много других вкусных вещей.

Али-Баба схватил курицу и мигом обглодал ее. Потом принялся за пилав, а покончив с ним, запустил руки в халву, но уже не мог съесть ни кусочка – до того он был сыт. Отдохнув немного, он осмотрелся и увидал вход в другую комнату. Али-Баба вошел туда – и зажмурил глаза. Комната вся сверкала и блестела – так много было в ней золота и драгоценностей. Золотые динары и серебряные дирхемы грудами лежали прямо на земле, словно камни на морском берегу. Драгоценная посуда – кубки, подносы, блюда, украшенные дорогими каменьями, – стояла по всем углам. Кипы шелка и тканей – китайских, индийских, сирийских, египетских –

лежали посреди комнаты; по стенам висели острые мечи и длинные копья, которых хватило бы на целое войско.

У Али-Бабы разбежались глаза, и он не знал, за что ему взяться: то примерит красный шелковый халат, то схватит золотой поднос и смотрится в него, как в зеркало, то наберет в пригоршню золотых монет и пересыпает их.

Наконец он немного успокоился и сказал себе:

– Эти деньги и драгоценности, наверное, награблены, и сложили их сюда разбойники, которые только что здесь были. Эти богатства не принадлежат им, и если я возьму себе немножко золота, в этом не будет ничего дурного. Ведь его здесь столько, что нельзя сосчитать.

Читателю. *Ошибка Али-Бабы состоит в том что он просто потерял голову Если уж вам посчастливилось добраться до цели – бегом забирайте то за чем вы пришли и обдумайте пути отхода!*

Али-Баба подоткнул полы халата и, встав на колени, стал подбирать золото. Он нашел в пещере два пустых мешка, наполнил их динарами, притащил к двери и крикнул:

– Симсим, открой дверь!

Дверь тотчас же распахнулась.

Али-Баба вышел из пещеры, и дверь захлопнулась за ним.

Колючие кусты и ветки переплелись и скрыли ее от глаз. Ослы Али-Бабы паслись на лужайке. Али-Баба взвалил на них мешки с золотом, прикрыл их сверху дровами и поехал домой.

Когда он вернулся, уже была ночь и встревоженная Зейнаб ждала его у ворот.

– Что ты делал в лесу так долго? – спросила она. – Я думала, что тебя растерзали волки или гиены. Отчего ты привез дрова домой, а не продал их?

– Сейчас все узнаешь, Зейнаб, – сказал Али-Баба. – Помоги-ка мне внести в дом эти мешки и не шуми, чтобы нас не услышали соседи.

Зейнаб молча взвалила один из мешков себе на спину, и они с Али-Бабой вошли в дом. Зейнаб плотно прикрыла за собой дверь, зажгла светильник и развязала мешок. Увидев золото, она побледнела от страха и крикнула:

– Что ты наделал, Али-Баба? Кого ты ограбил?

– Не тревожься, Зейнаб, – сказал Али-Баба. – Я никого не ограбил и сейчас расскажу тебе, что со мною сегодня случилось.

Он рассказал ей про разбойников и пещеру и, окончив свой рассказ, сказал:

– Смотри, Зейнаб, спрячь это золото и не говори о нем никому. Люди подумают, что мы и вправду кого-нибудь ограбили, и донесут на нас султану, и тогда он отнимет у нас все золото и посадит нас в подземелье. Давай выкопаем яму и спрячем туда золото.

Они вышли в сад, выкопали при свете луны яму, сложили туда все золото, а потом опять забросали яму землей.

Читателю. *Если уж вам довелось обладать тайной, то запомните, что то что знают двое – знают все!*

Покончив с этим делом, Али-Баба лег спать. Зейнаб тоже легла, но она еще долго ворочалась с боку на бок и думала:

«Сколько же золота привез Али-Баба? Как только рассветет, я пересчитаю все монетки до последней!»

На следующее утро, когда Али-Баба, как всегда, уехал на гору, Зейнаб побежала к яме, раскопала ее и принялась пересчитывать динары.

Но их было так много, что Зейнаб не могла сосчитать. Она не очень хорошо считала и все время сбивалась. Наконец это ей надоело, и она сказала себе:

– Лучше я возьму меру и перемеряю золото. Вот только меры у меня нет. Придется попросить у Фатимы.

Читателю. *Когда будете проводить расследование – помните, что главными слабостями человеческими являются жадность и глупость, что и подтверждается в сказке.*

А Касим с Фатимой жили в соседнем доме. Зейнаб сейчас же побежала к ним. Вошла в сени и сказала Фатиме:

– Сделай милость, одолжи мне ненадолго меру. Я сегодня же верну ее тебе.

– Хорошо, – ответила Фатима, – но моя мера у соседки. Сейчас я схожу за ней и дам ее тебе. Подожди здесь в сенях, у тебя ноги грязные, а я только что постлала чистые циновки.

Все это Фатима выдумала. И мерка, которой мерили крупу, висела на своем месте – в кухне, над очагом, и циновок она не меняла уже дней десять. На самом деле ей просто очень хотелось узнать, для чего Зейнаб вдруг понадобилась мерка, – ведь Фатима хорошо знала, что в доме у Али-Бабы давно уже нет никакой крупы. А спрашивать Зейнаб она не желала: пусть Зейнаб не воображает, что Фатима интересуется ее делами. И она придумала способ узнать, не спрашивая. Она вымазала дно мерки медом, а потом вынесла ее Зейнаб и сказала:

– На, возьми. Только смотри, не забудь возвратить ее в целости и не позже чем к закату солнца. Мне самой нужно мерить чечевицу.

Читателю *Если уж вам так не повезло, что инструменты для работы вы просите у соседа, то проверьте их на наличие злонамеренных вложений. И запомните на будущее – инструменты как и ложка должны быть свои.*

– Спасибо тебе, Фатима, – сказала Зейнаб и побежала домой. Она выгребла из ямы все золото и начала торопливо его мерить, все время оглядываясь по сторонам.

Золота оказалось десять мер и еще полмеры.

Зейнаб вернула мерку Фатиме и ушла, поклонившись ей до земли. Фатима сейчас же схватила мерку и заглянула в нее. И вдруг она увидела: ко дну мерки прилип какой-то маленький светлый кружочек. Это был новенький золотой динар.

Фатима не верила своим глазам. Она повертела монету между пальцами и даже попробовала ее на зуб: не фальшивая ли? Но динар был самый настоящий, из чистого золота.

– Так вот какая это крупа! – закричала Фатима. – Они такие богачи, что Зейнаб даже меряет золото мерой. Наверное, они кого-нибудь ограбили, а сами притворяются бедняками. Скорее бы Касим вернулся из лавки! Я непременно все расскажу ему. Пусть пойдет к Али-Бабе и пригрозит ему хорошенько! Али-Баба, наверное, поделится с ним.

Фатима весь день просидела у ворот, ожидая Касима. Когда стало смеркаться, Касим вернулся из лавки, и Фатима, не дав ему даже снять тюрбана, закричала:

– Слушай, Касим, какая у меня новость! Твой брат Али-Баба прикидывается бедняком, а он, оказывается, богаче нас с тобой!

– Что ты выдумала! – рассердился Касим. – Богаче меня нет никого на нашей улице, да и во всем квартале. Недаром меня выбрали старшиной рынка.

– Ты мне не веришь? – обиделась Фатима. – Ну, так скажи, как ты считаешь деньги, когда подсчитываешь по вечерам выручку?

– Обыкновенно считаю, – ответил Касим. – Складываю в кучки динары и дирхемы и пересчитываю. А как насчитаю сотню, загибаю палец, чтобы не ошибиться. Да что ты такие глупости спрашиваешь?

– Нет, не глупости! – закричала Фатима. – Ты вот считаешь динары на десятки и сотни, а Зейнаб, жена твоего брата, считает мерами. Вот что она оставила в моей мерке.

И Фатима показала ему динар, который прилип ко дну мерки.

Касим осмотрел его со всех сторон и сказал:

– Пусть меня не зовут Касимом, если я не допытаюсь, откуда у Али-Бабы взялись деньги. Хитростью или силой, но я отберу их у него!

Читателю. *Запомните, вы можете хотеть чего угодно, думать как угодно, но если чего-то захочет ваша жена, то вы сделаете это. Причем очень скоро. Даже если сами этого не хотите.*

И он сейчас же отправился к своему брату. Али-Баба только что вернулся с горы и отдыхал на каменной скамье перед домом. Он очень обрадовался Касиму и сказал:

– Добро пожаловать тебе, Касим! Ты не часто бываешь у меня. Что привело тебя ко мне сегодня, да еще в такой поздний час?

– Добрый вечер, брат мой, – важно сказал Касим. – Меня привела к тебе большая обида.

– Обида? – удивился Али-Баба. – Чем же мог я, бедный дровосек, обидеть старшину рынка?

– Ты теперь богаче меня, – сказал Касим. – Ты меряешь золото мерами. Вот что моя жена нашла на дне мерки, которую она одолжила твоей жене Зейнаб. Не обманывай меня: я все знаю! Почему ты скрыл от меня, что разбогател? Наверное, ты кого-нибудь ограбил?

Али-Баба понял, что Касим проведал его тайну, и решил во всем признаться.

– О брат мой, – сказал он, – я вовсе не хотел тебя обманывать. Я только потому ничего тебе не рассказал, что боялся воров и разбойников, которые могут тебя убить.

И он рассказал Касиму про пещеру и про разбойников. Потом протянул брату руку и сказал:

– О брат мой, мы с тобой оба – сыновья одного отца и одной матери. Давай же делить пополам все, что я привезу из пещеры. Я знаю, как туда войти и как уберечься от разбойников. Возьми себе половину денег и сокровищ – этого хватит тебе на всю жизнь.

– Не хочу половину, хочу все деньги! – закричал Касим и оттолкнул руку Али-Бабы. – Говори скорее, как войти в пещеру, а если не скажешь, я донесу на тебя султану, и он велит отрубить тебе голову.

– Зачем ты грозишь мне султаном? – сказал Али-Баба. – Поезжай, если хочешь, в пещеру, но только тебе все равно не увезти всех денег и сокровищ. Даже если бы ты целый год возил из пещеры золото и серебро, не отдыхая ни днем, ни ночью, – и тогда ты не увез бы и половины того, что там есть!

Он рассказал Касиму, как найти пещеру, и велел ему хорошо запомнить слова: «Сим-сим, открой дверь!»

Читателю. *Ну вот. Пароль передан. Он уже не секрет.*

– Не забуду, – сказал Касим. – Сим-сим… сим-сим… Это, кажется, растение, вроде конопли. Буду помнить.

Читателю. *Запомните пароль! Не можете запомнить – запишите и положите в надежное место, а лучше заведите себе менеджер паролей.*

На следующее утро Касим оседлал десять мулов, положил на каждого мула по два больших сундука и отправился в лес. Он пустил своих мулов пастись на опушке леса, отыскал дверь в скале и, встав перед нею, закричал изо всех сил:

– Эй, Сим-сим, открой дверь!

Дверь распахнулась. Касим вошел, и дверь снова захлопнулась за ним. Касим увидел пещеру, полную сокровищ, и совсем потерял голову от радости. Он заплясал на месте, потом бросился вперед и стал хватать все, что попадалось под руку, – охапки дорогих тканей, куски золота, кувшины и блюда, потом бросал их и срывал со стен золотые мечи и щиты, хватал пригоршнями деньги и совал их за пазуху. Так он метался по пещере целый час, но никак не мог забрать всего, что там было. Наконец он подумал:

«У меня времени много. Буду выносить отсюда мешок за мешком, пока не нагружу всех мулов, а потом приеду еще раз. Я буду ездить сюда каждый день, пока не заберу все, до последней монетки!»

Он схватил мешок с деньгами и поволок его к двери. Дверь была заперта. Касим хотел произнести волшебные слова, которые открывали дверь, но вдруг оказалось, что он позабыл их. Он помнил только, что надо сказать название какого-то растения. И он крикнул:

– Горох, открой дверь!

Но дверь не открылась. Касим немного испугался. Он подумал и крикнул опять:

– Пшеница, открой дверь!

Дверь и не шевельнулась. Касим от страха уже ничего не мог вспомнить и кричал названия всех растений, какие знал:

– Овес, открой дверь!

– Конопля, открой дверь!

– Ячмень, открой дверь!

Но дверь не открывалась. Касим понял, что ему никогда больше не выбраться из пещеры. Он сел на мешок с золотом и заплакал.

Читателю. *Как видите, Касим применяет классическую атаку по маске (растение). Однако атака по маске не всегда приносит удачу, особенно при недостаточной величине словаря.*

В это время разбойники ограбили богатых купцов, отобрали у них много золота и дорогих товаров. Они решили все это спрятать в пещере. Подъезжая к лесу, атаман заметил на опушке мулов, которые мирно щипали траву.

Читателю. *Если уж вы решили провести атаку, то заранее позаботьтесь о маскировке вашего мероприятия.*

– Что это за мулы? – сказал атаман. – К их седлам привязаны сундуки. Наверно, кто-нибудь разузнал про нашу пещеру и хочет нас ограбить!

Он приказал разбойникам не шуметь и, подойдя к двери, тихо произнес:

– Сим-сим, открой дверь!

Читателю. *Атаман в сложную минуту вспомнил инструкцию о снижении уровня сигнала и произнес пароль тихо. Но почему инструкцию нужно выполнять только в экстремальной ситуации?*

Дверь отворилась, и разбойники увидели Касима, который старался спрятаться за мешком с деньгами. Атаман бросился вперед, взмахнул мечом и отрубил Касиму голову.

Разбойники оставили тело Касима в пещере, а сами переловили мулов и, погнав их перед собой, ускакали.

А Фатима весь день просидела у окна – все ждала, когда покажутся мулы с сундуками, полными золота. Но время проходило, а Касима все не было. Фатима прождала день, прождала ночь, а утром с плачем прибежала к Али-Бабе.

Али-Баба сказал:

– Не тревожься, Фатима. Я сейчас сам поеду на гору и узнаю, что случилось с Касимом.

Он тотчас же сел на осла и поехал в лес, прямо к пещере. И как только вошел в пещеру, увидел, что его брат лежит мертвый на мешках с деньгами.

Али-Баба вынес тело Касима из пещеры, положил его в мешок и печальный поехал домой, думая про себя:

«Вот до чего довела Касима жадность! Если бы он согласился разделить со мной деньги и не захотел забрать себе их все, он и сейчас был бы жив».

Али-Баба устроил Касиму пышные похороны, но никому не сказал, как погиб его брат. Фатима говорила всем, кто провожал Касима на кладбище, что ее мужа растерзали в лесу дикие звери.

Когда Касима похоронили, Али-Баба сказал Фатиме:

– Знаешь что, Фатима, продай мне твой дом, и будем жить вместе. Тогда и мне не придется строить нового дома, и тебе не так страшно будет жить одной. Хорошо?

– О Али-Баба, – сказала Фатима, – мой дом – твой дом, и все, что у меня есть, принадлежит тебе. Позволь только мне жить с вами – больше мне ничего не нужно.

– Ну, вот и хорошо, – сказал Али-Баба, и они с Зейнаб и Фатимой зажили вместе.

Читателю. *Заранее подумайте кто вам предлагает помощь. И что он попросит за это. В данном случае Али-Баба воспользовался беспомощным положением Фатимы и забрал и ее и дом и все наследство. Если же предположить что Али-Баба заранее знал о плохой памяти и жадности Касима, то мы имеем классическую операцию по захвату бизнеса и имущества. Хотелось бы верить что это не так, но мы-то с вами безопасники, а значит должны думать о плохом, верно?*

Али-Баба еще несколько раз ездил в пещеру и вывез оттуда много золота, драгоценных одежд, ковров и посуды. Каждый день у него на кухне готовилась пища не только для него самого, Зейнаб и Фатимы, но и для всех его бедных соседей, которым нечего было есть. А когда соседи благодарили его, он говорил:

– Приходите и завтра и приводите с собой всех бедняков. А благодарить не за что. Я угощаю вас на деньги моего брата Касима, которого съели на горе волки. Он был богатым человеком.

Скоро все бедняки и нищие стали приходить к дому Али-Бабы к обеду и ужину, и жители города очень его полюбили.

Читателю, *Фактически Али-Баба подкупает электорат в надежде на будущие выборы. Однако получается что он мало того что грабит разбойников каждый день, так еще и скупает голоса для будущих выборов. Чем он отличается от разбойников? Да всего лишь умом и возможностью смотреть в будущее. Из таких вырастают современные политики и президенты!*

Вот что было с Али-Бабой, Зейнаб и Фатимой.

Что же касается разбойников, то они через несколько дней опять приехали к пещере и увидели, что тело их врага исчезло, а мешки с деньгами разбросаны по земле.

– В нашу пещеру опять кто-то заходил! – вскричал атаман. – Недавно я убил одного врага, но, оказывается, их несколько! Пусть не буду я Хасан Одноглазый, если я не убью всякого, кто хочет поживиться нашей добычей. Храбрые разбойники! Найдется ли среди вас смельчак, который не побоится отправиться в город и разыскать нашего обидчика? Пусть не берется за это дело трус или слабый! Только хитрый и ловкий может исполнить его.

Читателю. *Нет, все же атаман совсем глуп. И даже первый взлом не смог его научить ставить сигнализацию и охрану. Ну что стоило оставить пару разбойников в пещере? Нет. Решили сэкономить на охране и безопасности, вот и получили. Потому кто экономит на безопасности, того грабили и будут грабить!*

– О атаман, – сказал один из разбойников, – никто, кроме меня, не пойдет в город и не выследит нашего врага. Недаром зовут меня Ахмед Сорви-голова. А если я не найду его, делай со мной что хочешь.

– Хорошо, Ахмед, – сказал атаман. – Даю тебе один день сроку. Если ты найдешь нашего врага, я назначу тебя своим помощником, а если не найдешь – лучше не возвращайся. Я отрублю тебе голову.

– Будь спокоен, атаман, не пройдет дня, как ты узнаешь, где найти своего врага, – сказал Ахмед. – Ждите меня сегодня к вечеру здесь в лесу.

Он сбросил с себя разбойничье платье, надел синий шелковый халат, красные сафьяновые сапоги и тюбетейку и пошел в город.

Было раннее утро. Рынок был еще пуст, и все лавки были закрыты; только старый башмачник сидел под своим навесом и, разложив инструменты, ждал заказчиков.

Ахмед Сорви-голова подошел к нему и, поклонившись, сказал:

– Доброе утро, дядюшка. Как ты рано вышел на работу! Если бы я не увидел тебя, мне пришлось бы еще долго ждать, пока откроется рынок.

– А что тебе нужно? – спросил старый башмачник, которого звали Мустафа.

– Я чужой в вашем городе, – ответил Ахмед. – Только сегодня ночью я пришел сюда и ждал до рассвета, пока не открыли городские ворота. В этом городе жил мой брат, богатый купец. Я пришел к нему из далеких стран, чтобы повидать его, и, подходя к городу, услышал, что его нашли в лесу мертвым. Теперь я не знаю, как отыскать его родных, чтобы поплакать о нем вместе с ними.

– Ты говоришь, твой брат был богатый купец? – спросил башмачник. – В нашем городе недавно хоронили одного купца, и я был на похоронах. Жена купца говорила, что его растерзали волки, но я слышал от одного человека, что это неправда, а что этого купца на самом деле нашли в лесу убитым, без головы, и тайком привезли домой в мешке.

Ахмед Сорви-голова очень обрадовался. Он понял, что этот богатый купец и есть тот человек, которого убил атаман.

Читателю. *Классический пример социальной инженерии. Ну зачем тратить время и кого-то искать? Проще погулять и поговорить с соседями, сотрудниками… Ведь никто им не поясняет что делать.*

– Ты можешь меня провести к его дому? – спросил Ахмед башмачника.

– Могу, – ответил башмачник. – Но только как же мне быть с работой? Вдруг кто-нибудь придет на рынок и захочет заказать мне туфли, а меня не будет на месте?

– Вот тебе динар, – сказал Ахмед. – Возьми его за убытки, а когда ты покажешь мне дом моего брата, я дам тебе еще динар.

– Спасибо тебе за твою щедрость! – воскликнул обрадованный Мустафа. – Чтобы заработать этот динар, мне нужно целый месяц ставить на туфлях заплатки. Пойдем!

И башмачник привел Ахмеда к дому, где жил Касим.

Читателю. *Обратите внимание, вся операция обошлась совсем дешево.*

– Вот дом, где жил убитый купец. Здесь поселился теперь его брат, – сказал Мустафа.

«Его-то мне и надо!» – подумал Ахмед. Он дал Мустафе динар, и Мустафа ушел, кланяясь и благодаря. Все дома в этом городе были обнесены высокими стенами, так что на улицу выходили только ворота. Запомнить незнакомый дом было нелегко.

– Надо отметить этот дом, – говорил Ахмед сам себе, – чтобы потом узнать его.

Он вытащил из кармана кусок мела и поставил на воротах дома крестик. А потом пошел обратно и радостно говорил себе:

– Теперь я запомню этот дом и приведу к нему завтра моих товарищей. Быть мне помощником атамана!

Читателю. *Если уж вы ставите метку безопасности, позаботьтесь не только о ее уникальности. Продумайте вопрос ее скрытности. Иначе вам как бедному разбойнику, придется расплачиваться головой!*

Только Ахмед успел уйти, как из дома вышла служанка Али-Бабы по имени Марджана, девушка умная и храбрая. Она собралась идти на рынок за хлебом и мясом к обеду. Закрывая калитку, она обернулась и вдруг увидела на воротах крестик, нарисованный мелом.

«Кто это вздумал пачкать наши ворота? – подумала она. – Наверное, уличные мальчишки. Нет, крест слишком высоко! Его нарисовал взрослый человек, и этот человек задумал против нас злое дело. Он хочет запомнить наш дом, чтобы нас убить или ограбить. Надо мне сбить его с толку».

Марджана вернулась домой, вынесла кусок мела и поставила кресты на всех соседних домах. А потом ушла по своим делам.

Читателю. *Если вы не можете удалить какую-то сложную метку, поставьте ее и на соседние объекты. Таким образом вы сможете замаскировать свой объект.*

А разбойник прибежал в пещеру и крикнул:

– Слушай, атаман! Слушайте все! Я нашел дом нашего врага и отметил его крестом. Завтра я вам покажу его.

– Молодец, Ахмед Сорви-голова! – сказал атаман. – Завтра к утру будьте все готовы. Мы спрячем под халаты острые ножи и пойдем с Ахмедом к дому нашего врага.

– Слушаем и повинуемся тебе, атаман, – сказали разбойники, и все стали поздравлять Ахмеда с удачей.

А Ахмед Сорви-голова ходил гордый и говорил:

– Вот увидите, я буду помощником атамана.

Он всю ночь не спал, дожидаясь утра, и, как только рассвело, вскочил и разбудил разбойников. Они надели широкие бухарские халаты, белые чалмы и туфли с загнутыми носками, спрятали под халаты ножи и пошли в город. И все, кто их видел, говорили:

– Это бухарцы. Они пришли в наш город и осматривают его.

Впереди всех шел Ахмед с атаманом. Долго водил Ахмед своих товарищей по городу и наконец отыскал нужную улицу.

– Смотрите, – сказал он, – вот этот дом. Видите, на воротах крест.

– А вот еще крест, – сказал другой разбойник. – В каком же доме живет наш враг?

– Да вон и на том доме крест! И на этом! И здесь крест! Да тут на всех домах кресты! – закричали вдруг остальные разбойники.

Атаман рассердился и сказал:

– Что это значит? Кто-то перехитрил тебя, Ахмед! Ты не выполнил поручения, и не придется тебе больше с нами разбойничать. Я сам отрублю тебе голову!

И когда они вернулись в лес, жестокий атаман отрубил голову Ахмеду. А потом сказал:

– Кто еще возьмется отыскать дом нашего врага? У кого хватит храбрости? Пусть не пробует это сделать ленивый или слабый!

– Позволь мне попытаться, о атаман, – сказал один из разбойников, Мухаммед Плешивый. – Я – человек старый, и меня так легко не проведешь. А если я не исполню поручения, казни меня так же, как ты казнил Ахмеда.

– Иди, Мухаммед, – сказал атаман. – Буду тебя ждать до завтрашнего вечера. Но смотри: если ты не найдешь и не покажешь мне дом нашего врага, тебе не будет пощады.

На следующее утро Мухаммед Плешивый отправился в город. Ахмед рассказывал разбойникам про Мустафу, и Мухаммед прямо пошел на рынок к старому башмачнику. Он повел с ним такой же разговор, как и Ахмед, и пообещал ему два динара, если Мустафа покажет ему дом убитого купца. И Мустафа, обрадованный, довел его до самых ворот.

«Придется и мне как-нибудь отметить дом», – подумал Мухаммед. Он взял кусок кирпича, валявшийся на дороге, и нарисовал на воротах маленький крестик в правом верхнем углу.

«Здесь его никто не увидит, кроме меня, – подумал он. – Побегу скорей за атаманом и приведу его сюда».

И он быстро пошел обратно к своим товарищам. А Марджана как раз возвращалась с рынка. Увидев, что от ворот их дома крадучись отошел какой-то человек и побежал по дороге, она сообразила, что тут что-то неладно.

Марджана подошла к воротам, внимательно осмотрела их и увидела в правом верхнем углу маленький красный крестик.

«Так вот, значит, кто ставит кресты на наших воротах, – подумала Марджана. – Подожди же, я тебя перехитрю».

Она подняла с земли кусок кирпича и поставила такие же кресты на воротах всех домов их улицы.

Читателю. *Запомните, повторение одного и того же приема приводит к неудаче!*

– Ну-ка, попробуй теперь найти наш дом! – воскликнула она. – Тебе это так же не удастся, как вчера!

А Мухаммед Плешивый всю дорогу бежал, не останавливаясь, и наконец вошел в пещеру, еле переводя дух.

– Идемте скорее! – крикнул он. – Я так отметил этот дом, что уж теперь нашему врагу не уйти. Собирайтесь же скорее, не мешкайте!

Разбойники завернулись в плащи и пошли вслед за Мухаммедом. Они очень торопились, чтобы дойти до города засветло, и пришли туда перед самым закатом солнца. Найдя знакомую улицу, Мухаммед Плешивый подвел атамана к самым большим и красивым воротам и указал ему пальцем на маленький красный крестик в правом верхнем углу ворот.

– Видишь, – сказал он, – вот моя отметка.

– А это чья? – спросил один из разбойников, который остановился у соседних ворот. – Тут тоже нарисован крестик.

– Какой крестик? – закричал Мухаммед.

– Красный, – ответил разбойник. – И на тех воротах точно такой же. И напротив – тоже. Пока ты показывал атаману свой крестик, я осмотрел все соседние ворота.

– Что же, Мухаммед, – сказал атаман, – и тебя, значит, перехитрили? Хоть ты и хороший разбойник, а поручения не выполнил. Пощады тебе не будет!

И Мухаммед погиб так же, как и Ахмед. И стало в шайке атамана не сорок, а тридцать восемь разбойников.

«Надо мне самому взяться за это трудное дело, – подумал атаман. – Мои люди хорошо сражаются, воруют и грабят, но они не годятся для хитростей и обмана».

И вот на следующее утро Хасан Одноглазый, атаман разбойников, пошел в город сам. Торговля на рынке была в полном разгаре. Он нашел Мустафу-башмачника и, присев рядом с ним, сказал:

– О дядюшка, почему это ты такой печальный? Работы, что ли, мало?

– Работы у меня уже давно нет, – ответил башмачник. – Я бы, наверное, умер с голоду, если бы судьба не послала мне помощь. Позавчера рано утром пришел ко мне один щедрый человек и рассказал, что он ищет родных своего брата. А я знал, где дом его брата, и показал ему дорогу, и чужеземец подарил мне целых два динара. Вчера ко мне пришел другой чужеземец и опять спросил меня, не знаю ли я его брата, который недавно умер, и я привел его к тому же самому дому и опять получил два динара. А сегодня – вот уже полдень, но никто ко мне не пришел. Видно, у покойника нет больше братьев.

Услышав слова Мустафы, атаман горько заплакал и сказал:

– Какое счастье, что я встретил тебя! Я третий брат этого убитого. Я пришел с Дальнего Запада и только вчера узнал, что моего дорогого брата убили. Нас было четверо братьев, и мы все жили в разных странах, и вот теперь мы сошлись в вашем городе, но только для того, чтобы найти нашего брата мертвым. Отведи же меня к его дому, и я дам тебе столько же, сколько дали мои братья.

– Хорошо, – радостно сказал старик. – А больше у него нет братьев?

– Нет, – ответил атаман, тяжело вздыхая. – Нас было четверо, а теперь стало только трое.

– Жалко, что вас так мало, – сказал старый Мустафа и тоже вздохнул. – Идем.

Читателю. *Запомните, социальная инженерия это классика. Но применяйте различные ее приемы, не уподобляйтесь старым разбойникам, будьте умнее!*

Он привел атамана к дому Касима, получил свою плату и ушел. А атаман сосчитал и хорошо запомнил, сколько ворот от угла улицы до ворот дома, так что ему не нужно было отмечать ворота. Потом он вернулся к своим товарищам и сказал:

– О разбойники, я придумал одну хитрость. Если она удастся, мы убьем нашего врага и отберем все богатства, которые он увез из пещеры. Слушайте же меня и исполняйте все, что я прикажу.

И он велел одному из разбойников пойти в город и купить двадцать сильных мулов и сорок кувшинов для масла.

А когда разбойник привел мулов, нагруженных кувшинами, атаман приказал разбойникам влезть в кувшины. Он сам прикрыл кувшины пальмовыми листьями и обвязал травой, а сверху проткнул дырочки для воздуха, чтобы люди не задохнулись. А в оставшиеся два кувшина налил оливкового масла и вымазал им остальные кувшины, чтобы люди думали, что во всех кувшинах налито масло.

Сам атаман надел платье богатого купца и погнал мулов в город. Наступал вечер, уже темнело. Атаман направился прямо к дому Касима и увидел, что у ворот сидит человек, веселый и приветливый. Это был Али-Баба. Атаман подошел к нему и низко поклонился, коснувшись рукой земли.

– Добрый вечер, почтенный купец, – сказал он. – Я чужеземец, из далекой страны. Я привез запас дорогого масла и надеялся продать его в вашем городе. Но мои мулы устали от долгого пути и шли медленно. Когда я вошел в город, уже наступил вечер и все лавки закрылись. Я обошел весь город, чтобы найти ночлег, но никто не хотел пустить к себе чужеземца. И вот я прошел мимо тебя и увидел, что ты человек приветливый и радушный. Не позволишь ли ты мне провести у тебя одну ночь? Я сложу свои кувшины на дворе, а завтра рано утром увезу их на рынок и продам. А потом я уеду обратно в мою страну и буду всем рассказывать о твоей доброте.

– Входи, чужеземец, – сказал Али-Баба. – У меня места много. Расседлай мулов и задай им корму, а потом мы будем ужинать. Эй, Марджана, посади собак на цепь, чтобы они не искусали нашего гостя!

– Благодарю тебя, о почтенный купец! – сказал атаман разбойников. – Пусть исполнятся твои желания, как ты исполнил мою просьбу.

Читателю. *Конечно, людям нужно доверять. Но иногда, причем обязательно проверяя их при этом. Иначе…*

Он ввел своих мулов во двор и разгрузил их у стены дома, осторожно снимая кувшины, чтобы не ушибить разбойников. А потом нагнулся к кувшинам и прошептал:

– Сидите тихо и не двигайтесь. Ночью я выйду к вам и сам поведу вас в дом.

И разбойники шепотом ответили из кувшинов:

– Слушаем и повинуемся, атаман!

Атаман вошел в дом и поднялся в комнату, где уже был приготовлен столик для ужина. Али-Баба ждал его, сидя на низенькой скамейке, покрытой ковром. Увидя гостя, он крикнул Марджане:

– Эй, Марджана, прикажи зажарить курицу и приготовить побольше блинчиков с медом. Я хочу, чтобы мой гость был доволен нашим угощением.

– Слушаю и повинуюсь, – сказала Марджана. – Я приготовлю все это сама, своими руками.

Она побежала в кухню, живо замесила тесто и только что собралась жарить, как вдруг увидела, что масло все вышло и жарить не на чем.

– Вот беда! – закричала Марджана. – Как же теперь быть? Уже ночь, масла нигде не купить. И у соседей не достанешь, все давно спят. Вот беда!

Вдруг она хлопнула себя по лбу и сказала:

– Глупая я! Горюю, что нет масла, а здесь, под окном, стоят сорок кувшинов, с маслом. Я возьму немного у нашего гостя, а завтра чуть свет куплю масла на рынке и долью кувшин.

Она зажгла светильник и вышла во двор. Ночь была темная, пасмурная. Все было тихо, только мулы у колодцев фыркали и звенели уздечками.

Марджана высоко подняла светильник над головой и подошла к кувшинам.

И как раз случилось так, что ближайший кувшин был с маслом. Марджана открыла его и стала переливать масло в свой кувшин.

А разбойникам уже очень надоело сидеть в кувшинах скрючившись. У них так болели кости, что они не могли больше терпеть. Услышав шаги Марджаны, они подумали, что это атаман пришел за ними, и один из них сказал:

– Наконец-то ты пришел, атаман! Скорей позволь нам выйти из этих проклятых кувшинов и дай расправиться с хозяином этого дома, нашим врагом.

Марджана, услышав голос из кувшина, чуть не упала от страха и выронила светильник. Но она была умная и храбрая девушка и сразу поняла, что торговец маслом – злодей и разбойник, а в кувшинах сидят его люди и что Али-Бабе грозит страшная смерть.

Читателю. *Часовых как всегда губит курение на посту и болтовня. Веками говорят одно и тоже, но все равно мир полон беспечных болванов!*

Она подошла к тому кувшину, из которого послышался голос, и сказала:

– Скоро придет пора. Молчи, а то тебя услышат собаки. Их на ночь спустили с цепи.

Потом она подошла к другому кувшину и спросила:

– Кто тут?

– Я, Хасан, – ответил голос из кувшина.

– Будь готов, Хасан, скоро я освобожу тебя.

Так она обошла все кувшины и узнала, что в тридцати восьми кувшинах сидят разбойники и только в два кувшина налито масло.

Марджана схватила кувшин с маслом, побежала на кухню и нагрела масло на огне так, что оно закипело.

Тогда она выплеснула кипящее масло в кувшин, где сидел разбойник. Тот не успел и крикнуть – сразу умер. Покончив с одним врагом, Марджана принялась за других. Она кипятила масло на огне и обливала им разбойников, пока не убила всех. А затем она взяла сковородку и нажарила много румяных блинчиков, красиво уложила их на серебряное блюдо, облила маслом и понесла наверх в комнату, где сидели Али-Баба и его гость. Али-Баба не переставал угощать атамана разбойников, и скоро тот так наелся, что еле мог двигаться. Он лежал на подушках, сложив руки на животе, и тяжело дышал.

Али-Баба увидел, что гость сыт, и захотел повеселить его. Он крикнул Марджане:

– Эй, Марджана, спляши для нашего гостя лучшую из твоих плясок.

– Слушаю и повинуюсь, господин, – ответила Марджана с поклоном. – Позволь мне только пойти и взять покрывало, потому что я буду плясать с покрывалом.

– Иди и возвращайся, – сказал Али-Баба.

Марджана убежала к себе в комнату, завернулась в вышитое покрывало и спрятала под ним острый кинжал.

А потом она возвратилась и стала плясать.

Али-Баба и атаман разбойников смотрели на нее и качали головами от удовольствия.

И вот Марджана посреди танца стала все ближе и ближе подходить к атаману. И вдруг она, как кошка, прыгнула на него и, взмахнув кинжалом, вонзила его в сердце разбойника. Разбойник громко вскрикнул и умер.

Али-Баба остолбенел от ужаса. Он подумал, что Марджана сошла с ума.

– Горе мне! – закричал он. – Что ты наделала, безумная? В моем доме убит чужеземец! Стыд и позор на мою голову!

Марджана опустилась на колени и сказала:

– Выслушай меня, господин, а потом делай со мной, что захочешь. Если я виновата – убей меня, как я убила его.

И она рассказала Али-Бабе, как она узнала о разбойниках и как погубила их всех. Али-Баба сразу понял, что это те самые разбойники, которые приезжали к пещере и которые убили Касима.

Он поднял Марджану с колен и громко закричал:

– Вставай, Зейнаб, и разбуди Фатиму! Нам грозила страшная смерть, а эта смелая и умная девушка спасла всех нас!

Зейнаб и Фатима сейчас же прибежали и крепко обняли Марджану, а Али-Баба сказал:

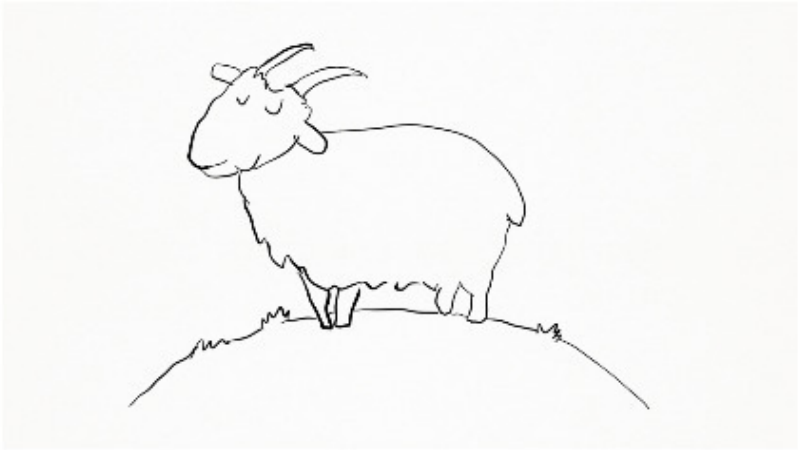
– Ты не будешь больше служанкой, Марджана. С этого дня ты будешь жить вместе с нами, как наша родная сестра.

И с этих пор они жили спокойно и счастливо.

PS

Надеюсь эти несложные приемы помогут вам понять, что и как нужно запомнить. Сказка ложь, да в ней намек!

ВОЛК И СЕМЕРО КОЗЛЯТ… УЧИМСЯ НА СКАЗКАХ, МАЛЫШИ!



Жила-была в красивом домике коза со своими семью козлятами…

– Никому не открывайте. Помните, что здесь неподалеку бродит злой волк. Сам он серый, лапы у него огромные и страшные, а голос злой и противный. Если он постучит, не открывайте!

Коза рисует портрет возможного нарушителя. Она не догадывается, что он может выглядеть и иначе! Но это типично для начинающего специалиста в ИБ. Помните! Нарушителем может быть ЛЮБОЙ! Даже тот, кому вы, безусловно, доверяете!

Когда она вышла из дома и остановилась поговорить о своих опасениях с соседкой, волк подслушивал, спрятавшись неподалеку.

Не болтайте о своих проблемах и планах, особенно в местах, не предназначенных для проведения совещаний. Оборудуйте комнату для ведения переговоров!

– Вот и хорошо! – сказал волк. – Раз коза идет на базар, то я пойду к ней домой и съем козлят.

Стараясь не попадаться никому на глаза, он пришел к домику козы и закричал своим страшным голосом:

– Отворитеся-отопритеся! Я ваша мама, я с базара пришла.

Обратите внимание, в отличие от прошлой сказки, здесь получения права войти в систему (в дом) используется уже многофакторная аутентификация. Получается что коза умнее разбойников? Факторы – тембр голоса и кодовая фраза.

Услышав грубый голос, козлята вспомнили наставления мамы (и говорят волку из-за закрытой двери: ***Учите пользователей правилам!!!)***

– Мы тебя узнали! Ты волк! У нашей мамы голосок нежный да сладкий, а не противный и грубый, как у тебя. Иди прочь, мы тебе никогда не откроем! (***Кодовая фраза совпала, тембр не подошел, второй фактор).***

И как ни стучал волк, козлята не открыли ему.

Тогда волк побежал к кондитеру и попросил у него пирог с медом. Волк надеялся, что от меда голос у него станет сладким, как у козы. И в самом деле, как только он проглотил пирог, ему показалось, что голос его и впрямь стал таким, как он хотел. (***Обратите внимание, используемые для аутентификации факторы должны быть неотчуждаемы! Т.е. если вы прозевали и ваш PIN-код смогли услышать, а затем подделать кредитную карту, вы же сами и виноваты. Вы никогда никому ничего не докажете!!!).***

И волк вернулся к домику.

– Отворитеся-отопритеся! Я ваша мама, я с базара пришла. Открывайте! – пропел он.

На этот раз козлята растерялись: уж очень голос был похож на мамин. Они уже собирались открыть дверь, как вдруг черный козленок засомневался:

– А покажи нам свою ножку, мама!

Ничего не подозревая, волк поднес лапу к окну, и козлята, увидев волосатую лапищу, поняли, что за дверью стоит волк.

– Ты не наша мама, у тебя такие страшные ножищи. Иди прочь, гадкий волк! – закричали они.

И на этот раз, как волк ни старался, дверь осталась запертой. (***Дополнительные рубежи проверки затрудняют взлом!!!)***

Тогда волк побежал на мельницу, нашел там мешок с белой мукой и запустил туда свои лапы, отчего они у него стали совсем белыми.

– Отворитеся-отопритеся! Я ваша мама, я с базара пришла. Открывайте!

Голос был похож на мамин, но недоверчивые козлята тут же попросили:

– Покажи нам свою ножку, мама!

Волк поднял белую, всю в муке, лапу, и козлята уверенно открыли дверь.

Если уж вы используете многофакторную аутентификацию с дополнительными рубежами проверки, постарайтесь уберечься от фальшивых ключей, сделайте их изготовление максимально сложным. Иначе сожрут вас, как волк козлят!

КОЛОБОК ИЛИ СТАРЫЕ СКАЗКИ О ГЛАВНОМ…

Жил-был старик со старухою.

Просит старик:

– Испеки, старуха, колобок.

– Из чего печь-то? Муки нету.

– Э-эх, старуха! По коробу поскреби, по сусеку помети; авось муки и наберется.

Взяла старуха крылышко, по коробу поскребла, по сусеку помела, и набралось муки пригоршни с две.

Замесила на сметане, изжарила в масле и положила на окошечко постудить.

Создали значит ИТ-отдел и поручили ему жить самостоятельно да добро наживать. Из последних сил тужились, чтобы было как у «людей». Да не тут-то было.

Колобок полежал-полежал, да вдруг и покатился – с окна на лавку, с лавки на пол, по полу да к дверям, перепрыгнул через порог в сени, из сеней на крыльцо, с крыльца на двор, со двора за ворота, дальше и дальше.

Решил ИТ-директор что он всех умнее и сам знает что нужно бизнесу, мол, чего их спрашивать, мы же ИТ, самые умные. И встретилась ему на большом пути первая опасность…

Катится колобок по дороге, а навстречу ему заяц:

– Колобок, колобок! Я тебя съем!

– Не ешь меня, косой зайчик! Я тебе песенку спою, – сказал колобок и запел:

– Я поскребён метен, на сметане мешон,

Я в масле пряжон, на окошке стужон;

Я от дедушки ушел, я от бабушки ушел,

От тебя, зайца, не хитро уйти!

И покатился себе дальше; только заяц его и видел!

Короче, опасность проигнорировали и исключили ее возникновение. Загордились сильно, а как же, мы ж мол вирусную атаку отразили (или еще от какой-то дряни спаслись), в конце-концов, почту работать заставили, вот какие умные

Впереди были еще две проблемы, но от них удалось ИТ-отделу увернуться. Ну как же собой не гордиться! Как же не хвастаться!

Однако и на старуху бывает своя проруха…

Катится, катится колобок, а навстречу ему лиса: – Здравствуй, колобок! Какой ты хорошенький!

А колобок запел…

– Какая славная песенка! – сказала лиса. – Но ведь я, колобок, стара стала, плохо слышу; сядь-ка на мою мордочку, да пропой еще разок погромче. Колобок вскочил лисе на мордочку и запел ту же песню. – Спасибо, колобок! Славная песенка, еще бы послушала! Сядь-ка на мой язычок да пропой в последний разок, – сказала лиса и высунула свой язык. Колобок сдуру прыг ей на язык, а лиса – ам его! – и скушала. ***Но… славная лиса владела основным приемом социальной инженерии – ЛЕСТЬЮ! И вот тут уже не выдержали ни ИТ отдел, ни ИБ. Всем хочется слышать какие они мудрые да какие незаменимые… Вот только не понимают, что чаще всего слышат эту лесть в последний раз!***

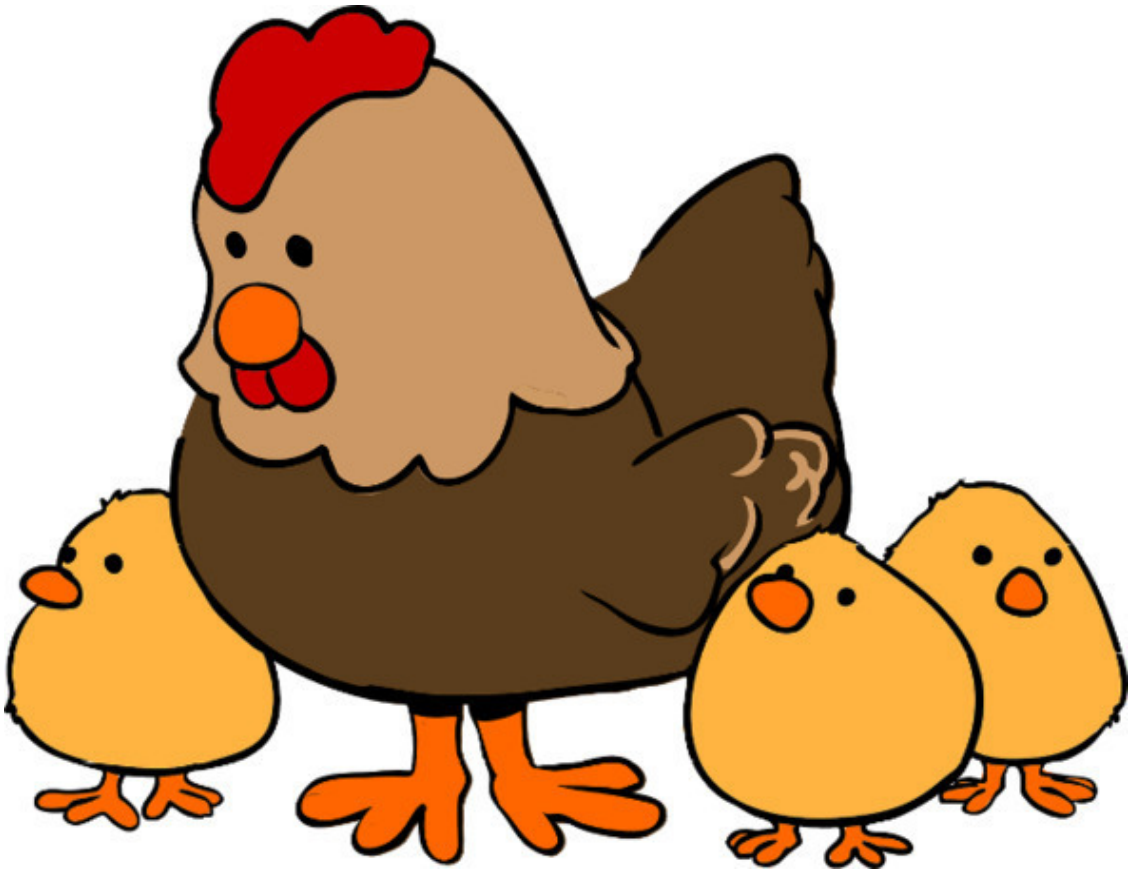
Вывод прост. ЕСЛИ ТЕБЯ ХВАЛИТ ПЕРВЫЙ ВСТРЕЧНЫЙ, ПОДУМАЙ, СМОЖЕШЬ ЛИ ТЫ РАСПЛАТИТЬСЯ ЗА ЭТУ ПОХВАЛУ…

PS

А СОТРУДНИКАМ ИБ НУЖНО ПОЧАЩЕ НАПОМИНАТЬ ПОЛЬЗОВАТЕЛЯМ ОБ ОПАСНОСТЯХ АТАК СОЦИАЛЬНОЙ ИНЖЕНЕРИИ. ВЕДЬ НА ДУРАКА

НЕ НУЖЕН НОЖ, ЕМУ С ТРИ КОРОБА НАВРЕШЬ И ДЕЛАЙ С НИМ ЧТО ХОШЬ! НО ЭТО УЖЕ ДРУГАЯ СКАЗКА.

Курочка ряба



Жили-были дед да баба. Была у них курочка ряба. Снесла курочка яичко, не простое – золотое.

Создали ИТ-систему. Не простую. А уж очень важную. И дорогую. И пригласили специалистов тестировать безопасность. Первая Tiger Team называлась Дед. И была она исключительно мужской

Дед бил, бил – не разбил.

Ничего не вышло у первой команды. То ли работали неправильно, то ли не то тестили. Но не успокоилось ИТ, решило попробовать другую команду – «Баба»

Баба била, била – не разбила.

И у этих ничего не вышло. Обрадовалось ИТ, решило руководство, что все хорошо, успокоилось. Да не тут-то было! Пришел непонятно откуда злоумышленник, которого не ждали, нашел самое слабое звено, ударил по нему и… Упала ИТ система! Упала! Рухнула!!!

Мышка бежала, хвостиком задела, яичко упало и разбилось.

Дед плачет, баба плачет, а курочка кудахчет:

– Не плачь, дед, не плачь, баба: снесу вам яичко не золотое – простое!

Вывод. Не стоит расслабляться, если при проверке вы не обнаружили уязвимых мест. Чаще всего это означает что вы просто не там искали! И помните! Прочность всей цепи равна прочности самого слабого звена! Ищите это слабое звено! НЕ РАССЛАБЛЯЙТЕСЬ!

Лиса и журавль или воспитание инсайдеров своими руками

В данной сказке мы с вами поговорим о том, как руководство фирмы своими руками воспитает инсайдеров, успешно убивая лояльность в своих сотрудниках

Лиса с журавлем подружились

Взяли толковых сотрудников ИТ и ИБ на работу в преуспевающую фирму. Руководство и так и эдак к ним. Давайте мол, не просто работать вместе, а дружить, мы ж такие хорошие и так вас любим. Но вот пришло время оплачивать успешно завершенный проект. И решило руководство распределять премию.

Вот вздумала лиса угостить журавля, пошла звать его к себе в гости:

– Приходи, куманек, приходи, дорогой! Уж я тебя угощу!

Пошел журавль на званный пир. А лиса наварила манной каши и размазала по тарелке. Подала и потчевает:

– Покушай, голубчик куманек, – сама стряпала.

Журавль стук-стук носом по тарелке, стучал, стучал – ничего не попадает!

А лисица лижет себе да лижет кашу, так все сама и съела.

Кашу съела и говорит:

– Не обессудь, куманек! Больше потчевать нечем.

Вот и распределили премию. Вся слава и премия досталась руководству (как обычно, впрочем), а ИТ досталось большое спасибо. Ну и понятно, зачем же с сотрудниками делить славу и деньги? Это и самому руководству пригодится…

И поняли сотрудники, что нечего им ждать от данного руководства. Ну и решили, что стоит ответить руководству той же монетой. Вот так и появляются инсайдеры

Журавль ей отвечает:

– Спасибо, кума, и на этом! Приходи ко мне в гости.

На другой день приходит лиса к журавлю, а он приготовил окрошку, положил в кувшин с узким горлышком, поставил на стол и говорит:

– Кушай, кумушка! Право, больше нечем потчевать.

Лиса начала вертеться вокруг кувшина. И так зайдет, и эдак, и лизнет его, и понюхает-то, – никак достать не может: не лезет голова в кувшин.

А журавль клюет себе да клюет, пока все не съел.

– Ну, не обессудь, кума! Больше угощать нечем!

Взяла лису досада. Думала, что наестся на целую неделю, а домой пошла – не солоно хлебала. Как аукнулось, так и откликнулось!

С тех пор и дружба у лисы с журавлем врозь.

Закончилась сказка не так красиво. ИТ отдел умудрился поставить в проекте логическую бомбу, а безопасники помогли им унести информацию. Вывод прост. Не стоит своими руками творить инсайдеров в своей организации. Господа руководители, помните, не стоит своими руками воспитывать себе врагов! Если вы зарабатываете, на своих сотрудниках, то помните, что выплатить премию вам обойдется гораздо дешевле, чем построить защиту от инсайдеров!!!

Лиса и козел или снова о пользе социальной инженерии

Бежала однажды лиса по дороге, засмотрелась на ворону и упала в колодец. Воды в колодце было немного: утонуть нельзя, но и выскочить – тоже нельзя.

Сидит лиса в колодце и думает, что делать? ***(Вот этим же вопросом зачастую задаются злоумышленники. Как сделать так, чтобы и информацию добыть и целым уйти.).***

В это время по дороге шел козел – умная голова. Заглянул в колодец и увидел там лису.

– Что ты там, лиса, делаешь?

– Отдыхаю, голубчик, – отвечает лиса. – Наверху жарко, а здесь прохладно, хорошо! Воды холодной – сколько хочешь! (***Заметьте, лиса ничего не предлагает. Она просто рекламирует свои услуги).***

А козел давно пить хотел.

– А хороша ли вода? – спрашивает козел.

– Отличная! – отвечает лиса. – Чистая, холодная! Прыгай сюда, если хочешь. Здесь и тебе, и мне место есть. ***(Реклама она и есть реклама. Жаль ведутся не только козлы… Или только?)***

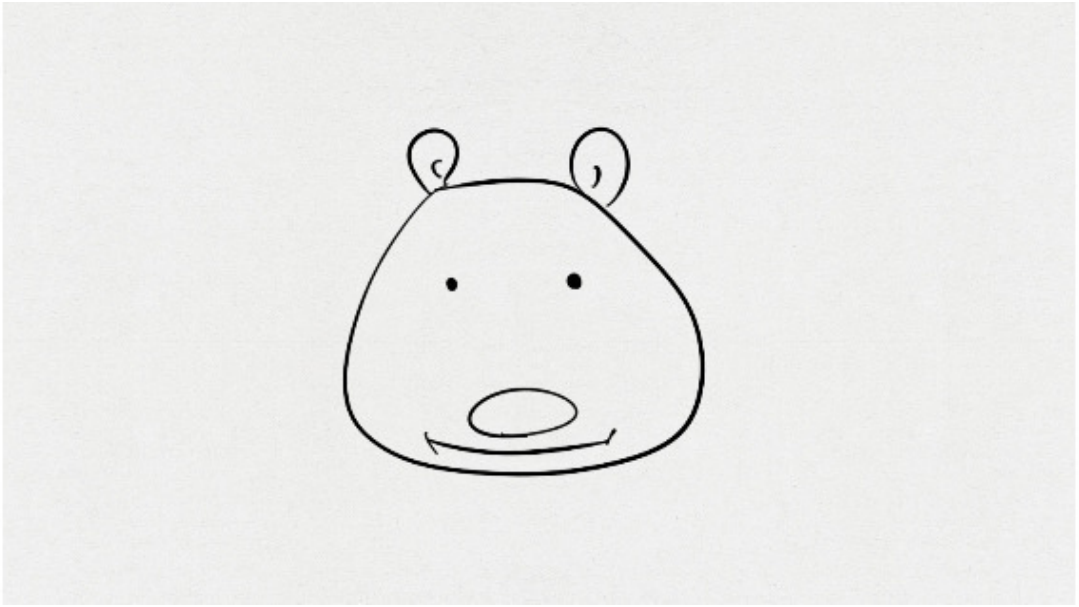
Прыгнул козел в колодец, а она ему говорит:

– Эх ты, и прыгнуть-то не умеешь – всю меня обрызгал.

Вскочила лиса козлу на спину, со спины на рога и выскочила из колодца. ***(Вот так, воспользовавшись нашей доверчивостью и восприимчивостью к рекламе и живут за наш счет!)***

А козел чуть было не умер с голоду в колодце. Еле нашли его и за рога вытащили. ***Повезло козлу. Но вам-то стоит учесть, что вы не козлы и может и не повезти. Причем куда чаще!***

Мужик и медведь или сказка о необходимости создания подразделения конкурентной разведки



Мужик поехал в лес репу сеять. Пашет там да работает (. *впрочем как и мы все. Работаем и работаем)*

Пришел к нему медведь (): *и тут без рэкета не обойтись!*

– Мужик, я тебя сломаю.

– Не ломай меня, медведюшка, лучше давай вместе репу сеять. Я себе возьму хоть корешки, а тебе отдам вершки.

– Быть так, – сказал медведь. – А коли обманешь, так в лес ко мне хоть не езди. *(А вот тут вылезает проблема отсутствия интернет-разведки у глупого мишки. Надеюсь у вас такое подразделение есть, чтобы понимать, а то ли вам предлагают что вы хотели?)*

Сказал и ушел в дуброву.

Репа выросла крупная. Мужик приехал осенью копать репу. А медведь из дубровы вылезает:

– Мужик, давай репу делить, мою долю подавай.

– Ладно, медведюшка, давай делить: тебе вершки, мне корешки.

Отдал мужик медведю всю ботву. А репу наклал на воз и повез в город продавать. (*Кто лежит на печи и ждет удачи, тем более не прилагая никаких усилий, того всегда бьет жизнь. Причем БОЛЬНО!)*

Навстречу ему медведь:

– Мужик, куда ты едешь?

– Еду, медведюшка, в город корешки продавать.

– Дай-ка попробовать – каков корешок? Мужик дал ему репу. Медведь, как съел:

– А-а! – заревел. – Мужик, обманул ты меня! Твои корешки сла-деньки. Тенерь не езжай ко мне в лес по дрова, а то заломаю. (*И опять понадеялся мишка на силу, да вот только глупых жизнь бьет. Неужели так и не понял, что прежде чем соглашаться на предложение, нужно внимательно составиь договор, оценить риски, провести разведывательные мероприятия).*

На другой год мужик посеял на том месте рожь. Приехал жать, а уж медведь его дожидается:

– Теперь меня, мужик, не обманешь, давай мою долю. Мужик говорит:

– Быть так. Бери, медведюшка, корешки, а я себе возьму хоть вершки.

Собрали они рожь. Отдал мужик медведю корешки, а рожь наклал на воз и увез домой.

Медведь бился, бился, ничего с корешками сделать не мог.

Рассердился он на мужика, и с тех пор у медведя с мужиком вражда пошла. (*Это вполне естественно. Дважды битый третий раз обманут не бывает. Хотя я на месте владельца конторы под названием «Медведь» еще после первого раза бы уволил весь менеджмент компании, но это уже тема другой сказки!)*

Красная шапочка

Жила-была одна девочка, которая почему-то очень не любила ходить прямым и коротким путем. Всегда она выбирала самую длинную и извилистую дорогу. А уж если мать посылала ее куда-нибудь с поручением, то ждать ее приходилась очень долго.

Помните, выбирая длинную дорогу, желая сделать по-своему, очень часто вы придете мало что не тогда, так еще и не туда.

Девочка часами могла бродить по окрестным лугам и лесам, собирать цветы и ягоды и напевать песенки. А еще она любила заговаривать с каждым, кто встречался ей на пути, даже совсем с незнакомыми. И часто случалось, что домой она возвращалась, лишь, когда уже вечерело. Но мать не ругала свою дочку, которая хотя никогда и не ходила короткой дорогой, но была девочкой доброй, приветливой и учтивой. Однако она очень беспокоилась, что девочка может заблудиться, и никто ее не найдет. Поэтому бабушка подарила внучке красную шапочку, чтобы она была видна даже издалека. И вскоре все, даже мать и бабушка, стали звать девочку Красной Шапочкой.

Как видите, идея со снабжением транспорта и особо ответственных машин маячками далеко не нова и издавна помогает в розыске транспортных средств. Главное, нужно чтобы соответствующая политика в организации однозначно определяла, что является важным средством и почему. А водителям (владельцам) данных средств о маячках знать совсем не обязательно!

Бабушка Красной Шапочки жила на другой стороне леса, через который к ее домику вела длинная извилистая тропинка. Каждую неделю Красная Шапочка вместе с матерью наве-

щали бабушку и приносили ей корзинку с гостинцами. Бабушка очень любила свою прелестную внучку и каждый раз с нетерпением ожидала ее, сидя у окошка, и, едва завидев, радостно махала рукой.

Но однажды бабушка заболела, и нужно было срочно отнести ей настойку из лесных ягод. Мать Красной Шапочки была очень занята по хозяйству и не могла сама навестить бабушку. А отправлять Красную Шапочку одну она боялась. Наверняка девочка свернет с тропинки, станет собирать цветы и забудет обо всем на свете. А вдруг она не успеет добраться к домику бабушки засветло? Ведь ночью никто не увидит ее красной шапочки, и она заблудится в лесной чаще.

Что же делать? Бабушка была очень больна, и только настойка из лесных ягод могла вылечить ее. Тогда мама решила пойти на хитрость. Она позвала Красную Шапочку и сказала:

Главное в жизни – инструктаж! И иногда стоит даже припугнуть пользователя, ведь лучше его испугать чтобы он не совершал ошибок. Но не стоит этим злоупотреблять, иначе толку никакого!

– Послушай, Красная Шапочка, ты пойдешь сегодня одна к бабушке. Девочка от радости захлопала в ладоши.

– Но сперва я должна сказать тебе что-то ужасное. Знай, что в нашей округе объявился злой волк.

Она взглянула на Красную Шапочку, не испугалась ли она?

– Волк? – удивилась Красная Шапочка. – А кто это такой?

– Глупенькая, это страшный зверь. Он рыщет в темном лесу и ищет маленьких девочек, которые не ходят короткой дорогой.

Красная Шапочка не на шутку испугалась.

– Но ты можешь легко избежать встречи с ним, – сказала мама, – иди по тропинке и никуда не сворачивай. И главное – нигде и ни с кем не останавливайся.

– Тогда я не пойду одна, – испуганно прошептала девочка.

– Но кто-то ведь должен отнести больной бабушке настойку из лесных ягод, а я не могу сегодня оторваться от дел. Не бойся. Если будешь делать все так, как я тебе сказала, тебе нечего бояться волка.

Красная Шапочка послушно взяла корзинку, куда мама положила настойку из лесных ягод, баночку варенья и пирог со сливами, и вздохнула. Девочка очень любила свою бабушку, и болезнь той огорчала ее, но ей совсем не хотелось идти одной через лес, где рыскал злой волк.

Красная Шапочка быстро, стараясь не смотреть по сторонам, пошла по лесной дорожке. Кругом росли очень красивые цветы, но она на них даже не глядела. День был чудесный. Птицы порхали с ветки на ветку и удивлялись, почему это маленькая подружка даже не замечает их. А Красной Шапочке было не до них. Она шла и говорила самой себе: «Уже недалеко, осталось пройти совсем немножко». Но что это краснеет там у тропинки? Какая спелая земляничка! Красная Шапочка уже собиралась пройти мимо, но вспомнила, что мама ничего не говорила о землянике. Девочка остановилась, наклонилась и сорвала с кустика одну ягодку. Ничего страшного не случилось. Волка нигде не было видно. Только птички продолжали петь в верхушках деревьев и колыхались цветы в зеленой траве. Красная Шапочка никогда еще не ела такой сладкой земляники. Жалко, что здесь росла только одна ягодка.

Ой, нет! Шагнув в сторону, Красная Шапочка нашла еще один кустик земляники, потом второй, третий.

Девочка совсем забыла о своем страхе и о злом волке. Собирая спелые и сладкие ягоды, она заходила все дальше и дальше в лес.

Учтите, инструктируя пользователей мало рассказать, чего вы от них хотите, нужно провести экзамен, чтобы понять, как они поняли ваш инструктаж!

– Здравствуй, девочка, – услышала она вдруг за спиной.

Красная Шапочка обернулась и увидела лохматое, но выглядевшее вполне добродушно существо.

– Ой, как вы меня напугали. Я уж думала, что вы и есть тот самый страшный волк.

Волк хихикнул про себя. Никогда еще не случалось такого, чтобы его кто-то не узнал.

– Какой же я волк! Я всего лишь скромный лесной обитатель. А куда ты идешь с этой корзинкой?

– Я очень спешу к своей бабушке. Она заболела, и я должна отнести ей лекарство.

Волк, который поначалу хотел сразу съесть девочку, неожиданно передумал.

– А где живет твоя многоуважаемая бабушка?

– Сразу за лесом, там, где кончается тропинка.

Только она это сказала, как волк скрылся за деревьями и что было духу побежал прямо к домику бабушки.

Поясняйте вашим детям, впрочем, и взрослым тоже, что не стоит говорить куда и зачем вы идете (едете), незнакомым людям. И уж те более не стоит рассказывать об этом всему белому свету в социальных сетях (Facebook, Instagram, Вконтакте и т.д.). Расплата может быть не только мгновенной, но и весьма болезненной.

Красная Шапочка слегка удивилась, что лохматый господин ушел не попрощавшись, но времени на раздумья у нее не было.

Вспомнив о мамином наказе, она отыскала тропинку и, боязливо оглядываясь по сторонам, зашагала дальше.

Тем временем волк, который побежал через лес напрямик, прибежал к домику бабушки и постучал три раза.

– Кто там? – спросила бабушка слабым голосом.

– Это я, твоя внучка Красная Шапочка, – ответил Волк.

– Входи, детка.

Если уж вы не можете сами проверить кто там за дверью, продумайте процедуру аутентификации. Либо, уважаемые взрослые дети, помогите вашим престарелым родителям, поставьте им в квартире систему видео, чтобы видели кто за дверью. Естественно, замаскируйте ее. В самом крайнем случае продумайте систему паролей (как для детей, так и для взрослых. Ну думайте же!

Волк ворвался в домик и, прежде чем бабушка успела опомниться, в один миг проглотил ее. Потом нацепил бабушкин чепчик, улегся на ее кровать и натянул по уши одеяло. Вскоре к домику подошла Красная Шапочка и, ничего не подозревая, постучала в дверь.

– Бабушка, это я, твоя Красная Шапочка! Я принесла тебе настойку из лесных ягод, варенье и пирог.

– Дверь открыта! – прорычал хриплым голосом Волк. Красная Шапочка вошла в дом и, увидев бабушку, очень удивилась.

– Бабушка, какой у тебя грубый голос!

– Конечно грубый, ведь я больна, – прохрипел Волк. – Подойди ближе, дитя мое.

Красная Шапочка поставила корзинку с гостинцами на пол и боязливо приблизилась. Уж очень странно выглядела сегодня бабушка.

Та же ошибка аутентификации. Но на этот раз Красная Шапочка не может проверить, а действительно ли это ее бабушка. Как видите, биометрическая аутентификации (по тембру голоса) не сработала. Нужен другой фактор.

– Ой, бабушка, какие у тебя большие руки!

Волк поскорее спрятал лохматые лапы под одеяло.

– Это чтобы покрепче обнять тебя, Красная Шапочка! Подойди-ка поближе.

– Но бабушка, почему у тебя такие большие уши?

– Чтобы лучше слышать тебя, Красная Шапочка. Ну, сядь ко мне.

– Ой, бабушка, почему у тебя такие большие глаза?

– Чтобы лучше видеть тебя, Красная Шапочка, – нетерпеливо буркнул Волк.

– Ой, бабушка, – закричала Красная Шапочка, пятясь назад, – почему у тебя такие большие зубы?

– Чтобы скорее съесть тебя! – прорычал Волк, выскочил из-под перины, щелкнул зубами и проглотил девочку вместе с ее красной шапочкой. Потом он улегся обратно в кровать и захрапел.

Как видите, биометрия не сработала. Потому или заранее вырабатывайте четкие критерии биометрической аутентификации или продумайте заранее что-то в дополнение к биометрии. Ведь не зря же компания Microsoft считает биометрию удобством, а не средством аутентификации.

К счастью, мимо проходил лесник. Он уже издали заметил, что случилось что-то неладное: двери домика были распахнуты настежь, и оттуда доносился громкий храп. Лесник снял с плеча двустволку и подкрался к окну. Он чуть не вскрикнул, увидев развалившегося на бабушкиной кровати волка с вздувшимся брюхом. Не раздумывая, лесник вбежал в дом, выхватил из-за пояса охотничий нож и мгновенно распорол волку брюхо. Оттуда выскочила Красная Шапочка, а за ней и бабушка. Ох, как темно было в брюхе у волка! Страшно даже подумать, что бы было, не приди храбрый и находчивый лесник вовремя.

К сожалению, вам стоит усвоить, что чаще всего лесники приходят тогда, когда уже поздно и даже если злоумышленник будет наказан, вам от этого легче не станет.

С тех пор они жили счастливо. В лесу больше не водились злые волки, и по тропинке можно было ходить, никого не боясь. Красная Шапочка могла теперь сколько угодно останавливаться по дороге и даже гулять в темном лесу. Однако теперь она этого больше не делала: с той поры она всегда ходила самой короткой дорогой.

Все верно, пользователи наиболее хорошо усваивают правила, связанные с собственными ошибками, да вот только стоит усвоить заранее, лучше учиться на чужих ошибках. На своих уж больно дорого, да и просто больно!

Сказки о безопасности: Рыцарь и Дракон, или как была изобретена двухэтапная аутентификация

Жил да был на свете рыцарь. Не слишком умный, не слишком храбрый, все в нем было в меру.

Ну, а где вы видели идеального героя? В сказке? Искать идеального специалиста можно долго и упорно. Но вот найти его можно уж точно только в сказке.

Надоело ему шляться по свету, решил он, что пора бы и жениться. Но жена должна быть не просто умная и красивая. Неплохо бы и приданое побольше.

Уж поверьте, даже в сказках герои бывают не только умными и сильными, но и практичными. Читателю.

Ездил он по белу свету, искал себе невесту. И вот однажды наткнулся на заколдованный замок Дракона, стоявший в темном-темном лесу. Впрочем, может, лес показался темным-темным, потому как наступил вечер. Объехав замок, Рыцарь увидел, что в стенах нигде нет и намека на ворота. Что ж делать? Решил он остаться до утра, а там посмотрим.

Как я уже говорил, Рыцарь был весьма практичным человеком и понимал, что шляться в незнакомом месте, да еще и ночью, без разведки местности – так можно и шишки набить. И вам, дорогие мои читатели, советую того же. Прежде чем начинать любую работу, осмотритесь, сможете ли вы что-то полезное сделать? А не сможете – не беритесь. Читателю.

Настало утро. Прилетел Дракон. И закричал он громовым голосом: «Открывайте дверь, хозяин пришел!» И открылись вдруг ворота.

Какую типичную ошибку совершил Дракон? Он воспользовался общедоступным каналом беспроводной связи для передачи пароля. Мало того, он орал во все горло. А ведь чего проще? Подойди к замку и скажи то же самое шёпотом. Т. е. вот вам первый урок – необходимо снизить уровень сигнала в беспроводной сети до минимально необходимого. И уж если пользуетесь беспроводной сетью для передачи пароля, используйте одноразовые пароли – One Time Password. Читателю.

Но Дракон он и есть Дракон…

Наелся, напился, выспался и улетел по своим делам. Решил Рыцарь попробовать. Подошел он к замку и заорал: «Открывайте дверь, хозяин пришел!» И открылись вдруг ворота.

Зашел Рыцарь, пробежался по кладовым, награбил золота, забежал в главную башню, забрал принцессу и убежал. Если вы думаете, что он стал ждать Дракона и вызывать его на бой, то вы ошибаетесь. Зачем? Я ж говорю, что он был практичным. Золото взял, принцессу освободил, а Дракон, – да кому он нужен, Дракон? Пусть его следующий рыцарь убивает.

Вовсе не обязательно убивать Дракона. Ведь вы не идеалист? И животных любите, экологию уважаете. А Дракон? Да кому он нужен, Дракон? Главное – золото и принцесса ваши. Именно так и думает злоумышленник. Кому нужны ВСЕ ваши тайны? Достаточно одной, чтобы обеспечить вам беспокойную жизнь. Потому не пытайтесь охранять все одинаково тщательно. Выберите, что важнее – принцесса или золото. Читателю.

Прилетел Дракон. Скажем мягко, расстроился. Но ненадолго. Нашел он себе другую принцессу и повелел ей каждый раз, когда она услышит фразу: «Открывайте дверь, хозяин пришел!», садиться у окна и кричать одну строку из длинного списка, который дал ей Дракон. Каждый раз следующую. Но только если она увидит Дракона из окна.

Сам же Дракон повторял эту строку и только после этого открывались ворота. Так была изобретена первая в мире двухэтапная аутентификация.

Сказки о безопасности: Королевский арсенал, или проводите аудит вовремя

В дальней-дальней стране жил да был король. Он обожал оружие и собирал его по всему свету. Да вот беда, насобирал он его так много, что уже и сам запутался, что есть у него, а чего нет. Никто и никогда не пытался навести порядок в его оружейном арсенале.

Надеюсь, вы понимаете, что собирать оружие (программное обеспечение), конечно, можно, но при этом необходимо понимать, что вы собираете, как будете его применять и ради чего, собственно. Читателю.

Проблемой короля было отсутствие элементарного учета. Одно время учет пытался организовать его министр финансов, ведь на это тратились деньги, но ничего хорошего из этого не вышло. Ведь каждый раз получалось примерно следующее: «Экспонат №1. Большая палка с железным наконечником».

Не правда ли, похоже на учет ПК в бухгалтерии. «Куплен ПК фирмы Dell. Инвентарный №…» Пользы от такого учета, естественно, никакой. Более того, только вред. Потому как понять, что за ПК, какие комплектующие, для чего может применяться, а главное – достаточно ли данного ПК для выполнения тех или иных задач – невозможно. Читателю.

Пришел к королю новый командующий войсками и ужаснулся. Вроде как все есть, оружия полно, но где и что? А тут еще приказ короля – маневры. Но поскольку в королевстве маневров отродясь не было, то пришлось солдатам и офицерам себе оружие выбирать. Неделю провозились, а дальше арсенала никто и не вышел. Не могут понять, что кому брать с собой. Название вроде есть, а оружия вроде и нет.

– Я пикинер, – кричал пожилой сержант, – но это же никакая не пика! Тут написано «Большая палка с железным наконечником»!

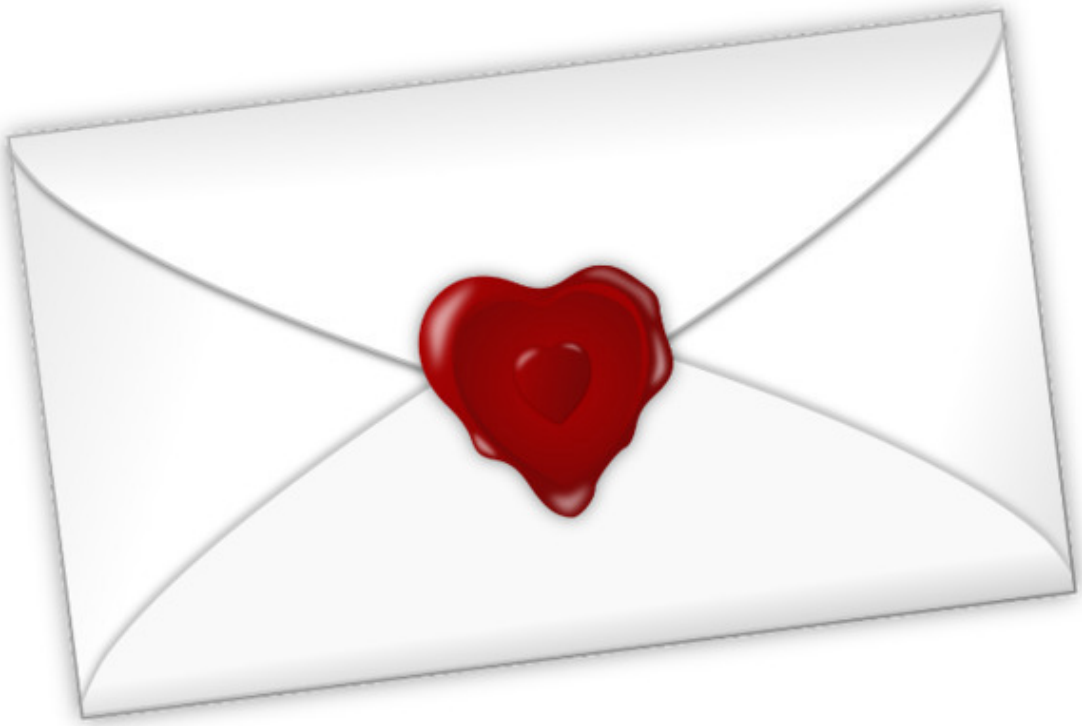
– А где мои доспехи?! – шумел рыцарь. – Тут стоит «Железный доспех, мастер Адобини», а на деле – тридцать пар наколенников!

Пришлось командующему целый год просто наводить порядок, пересчитывая и разбираясь что же у него есть, что нужно отремонтировать, а что просто выбросить и купить новое. И только наведя порядок, можно было организовать оборону.

Вам это ничего не напоминает? Когда в вашей организации в последний раз проводился аудит аппаратного и программного обеспечения? Вы, как руководитель ИТ (ИБ) знаете, что в вашей организации требует замены (улучшения)? И, безусловно, у вас есть календарный план замены (обновления) аппаратуры и программного обеспечения? И вы регулярно обновляете ПО не только от Microsoft, но и других производителей? Вот видите сколько вопросов. А всего лишь нужно регулярно проводить аудит. Читателю.

Со временем удалось навести порядок не только в оружейной, но и в королевстве. И не только навести порядок, но и организовать обучение по наведению порядка для других королевств и княжеств и этим существенно пополнил казну

Сказки о безопасности: И королям нужна почта



Жил да был король. И пришло ему время идти в поход. Соседнее королевство войну ему объявило. И решил король, что будет он ежедневно гнать гонца с новостями для советников. Создал он для этого сеть почтовых станций, чтобы гонцы могли лошадей менять.

Долго длился поход, и решили советники брать власть в свои руки. Как это сделать проще всего? Для начала нужно читать королевскую почту до того, как она официально будет зачитана.

Не правда ли, стандартный сценарий переворота? Кто владеет информацией – владеет миром! Пора бы вам усвоить, что самое ценное в мире – это информация. Читателю.

Как решили, так и сделали. На последней станции перед столицей гонца накормили-напоили, подсыпали ему снотворное, а пока гонец спал, пакет вскрыли и прочли.

Нельзя посылать важные данные в незашифрованном виде, иначе вы рискуете тем, что они станут известны злоумышленникам! Читателю.

Мало того, решил советник подменять письма. Как решил, так и сделал.

Для важных писем необходимо использовать подпись. Если вы пересылаете письмо в электронном виде, используйте электронную подпись. Иначе вам сложно будет доказать, что вы не писали это письмо или писали совершенно иное. Читателю.

Показалось странным королю, что делается совсем не то, о чем он говорит. И решил король, что почту его читает враг. Решил он использовать шифрование. Но тут возникает главная проблема – как передать ключ?

Так как король все же учился в школе так себе, король же, то решил он доверить ключ шифрования гонцу.

Кончилось все это так же печально. Гонца напоили, подкупили и он передал ключ шифрования советнику.

Я надеюсь, что вы все же образованнее сказочного короля и понимаете, что ключи шифрования нужно пересылать по другому каналу связи. Запомните! Никогда не передавайте ключи тем же каналом. То есть, отправляя письмо электронной почтой, ключи отправляйте, например, с помощью SMS. Никогда не доверяйте передачу пароля (ключа) человеку. Человек слаб, и это нужно помнить. Читателю.

В сказке все закончилось хорошо. Король вернулся из похода и наказал советника. Но учтите, жизнь, увы, далеко не сказка и закончиться тут может все гораздо страшнее!

Сказки о безопасности: Король и охрана, или о корпоративной службе безопасности

Жил да был король в королевстве. Хоть оно и маленькое, да все ж свое. Старался он не воевать особо, да враги все же были.

Каким бы хорошим вы ни были, да ведь все равно всем не угодишь. Рано или поздно находится желающий ваше королевство отобрать, а вас отправить куда подальше. И хорошо если живым. Читателю.

Так и случилось. Поднялся в королевстве мятеж. Мятежников удалось разгромить, но задумался король, что непорядок это. Нужна в королевстве служба безопасности. Создали такую службу. Да вот где взять руководителя? Думал король, думал, да и решил назначить графа. Неважно, как его звали, назовем просто Граф.

В чем была ошибка короля? А ошибка, в общем-то была типичной. Поиск руководителя СБ король доверил известной компании хедхантеров. А им-то что? Нашли и ладно. А ведь очень немногие из руководителей понимают, что безопасность мало создать. Ею надо управлять. Управлять эффективно и безопасно. Для этого надо отчетливо понимать, какие приказы и когда можно давать безопаснику (приказ должен быть своевременным, полным и выполнимым), всегда знать, чем занят безопасник, как он это делает и самое главное – зачем. Читателю.

Трудно пришлось Графу налаживать работу. Ведь до его появления команда управленцев короля уже сложилась.

С одной стороны, введение СБ помогло королю понять, что и как творится в государстве, понять почему, например, наместник Южного Округа все время жалуется на недостаток средств, а сам живет, пожалуй, богаче короля, а с другой, роптать стали управленцы, мол, СБ лезет во все дыры и работать мешает.

Как правило, внедрение сотрудниками Службы различных контрольных и проверочных процедур нарушает устоявшиеся производственные взаимосвязи. В такой ситуации СБ встречает неприязненное отношение со стороны персонала, и нередко в таких случаях можно слышать недовольный ропот: «И без них нормально работали, явились нахлебники и т. д.» Читателю.

Но рано или поздно, а штат нужно расширять. И решил король, – пусть сам начальник СБ собирает себе команду, да только если что-то пойдет не так, он сам отвечает головой за своих сотрудников.

Наиболее оптимальным представляется такой вариант: руководителя службы следует принимать на работу только по рекомендации хорошо знакомых вам лиц. Комплектование службы следует поручить руководителю СБ, поставив ему основное условие – он отвечает за каждого приглашенного им сотрудника, как за себя самого. При таком варианте комплектования СБ можно не волноваться за вопросы сплоченности коллектива, отпадает период взаимной притирки сотрудников, низка вероятность внутренних конфликтов, высока степень взаимного доверия сотрудников. Читателю.

И с тех пор в королевстве забыли и думать о мятежах. Все стало тихо и спокойно. Да вот только все равно беспокойно спит король. А что если предаст начальник СБ? Но это уже тема другой сказки.

Сказки о безопасности: Король и фишинг

В дальнем государстве жил да был король и решил он для блага подданных ввести в государстве почту. Сказано-сделано! И вот уже по дорогам королевства покатили почтовые кареты. От станции к станции катят кареты. На станциях сделаны комнаты для отдыха гонцов. Все вроде бы хорошо.

Но как-то раз пришла почта королю. В полученном письме говорилось что отец короля задолжал соседу 5000 золотых. И была приложена копия расписки.

Задумался король. Вроде и деньги не сильно велики, да не говорил ему отец ни о каких долгах. Решил позвать король министра финансов.

– Министр, что ты знаешь о долге моего отца?

– О каком долге, ваше величество? У вашего отца не было долгов!

Король протянул письмо министру. То стал изучать и конверт и письмо, а потом расхохотался: «Ваше величество! Вас пытались провести как мальчишку на рынке! Смотрите, здесь шнурок не того качества, не шелковый, печать не та, да и подпись странная.»

Присмотрелся король. Все верно. Прав министр! Но нужно убедиться все же. И отправил король гонца по указанному адресу. Своего, особого, королевского. Убедился гонец, что нет там такого отправителя.

Читателю. Запомните, если вы и хотите убедиться, что ваш адресат не слал вам никакого письма, попробуйте запросить подтверждение другим каналом связи, т.е. если вам пришло письмо – отошлите SMS или перезвоните, ведь основной канал может быть скомпрометирован.

Так была отражена первая фишинговая атака в истории королевства.

Запомните, прежде чем платить или пересылать запрашиваемую конфиденциальную информацию, убедитесь, что отправитель действительно ваш знакомый. Причем убедитесь по стороннему каналу связи. И еще. Для банковских приложений. Банк никогда не будет присылать вам запросы о ваших действиях. Никогда банк не может запросить у вас ваш номер кредитной карты, CVV и т. д. Будьте внимательнее! Читателю.

Сказки о безопасности: Как в королевстве справились с эпидемией, или об общедоступном бета-тестировании

В дальнем-дальнем королевстве был богатый портовый город О. Из этого города морские суда частенько хаживали за море и привозили разные заморские диковинки: овощи, фрукты, заморские вина. Все это стоило сравнительно недорого, поэтому рынки и ярмарки ломились от заморского товара, а в самом городе его можно было попробовать даже в недорогих приморских ресторанчиках.

Но так продолжалось недолго. Вдруг в городе разразилась эпидемия неизвестной болезни. Люди начали болеть и даже умирать. Никто не мог понять, откуда в город пришла зараза.

Увы, но беда всегда приходит вдруг. Тем и отличаются мудрые руководители, что заранее готовы к наступлению неприятностей. А вы готовы? У вас существует план непрерывности бизнеса? Есть документы, которые регламентируют работу в случае чрезвычайной ситуации? Нет? Значит самое время обратить на это внимание! Читателю.

Долго болели люди. Но наконец-то в город пришел Врач. Он долго бродил по городу, беседовал с больными и здоровыми и пришел к Правителю. О чем они беседовали, мне неведомо. Да только Правитель издал Указ, согласно которому в городе:

Запрещено торговать заморскими новинками, которые начали ввозить в город в последние пять лет.

Создаются таверны для бедных, в которых за счет города кормят неимущих и желающих заморскими товарами и заморским вином, которые начали ввозить в последние пять лет.

Таким образом в городе организовывается две зоны – чистая (белая), в которой еда и питье проверены и не содержат заразы. И серая, в которой еда и питье могу содержать заразу и подлежат проверке на нищих и добровольцах. То есть реализован принцип Default Deny (Whitelisting, белый список). Читателю.

Еда и питье, впервые ввозимые в город, тестировались на специально отобранных бесполезных рабах, которые сами уже не могли ничего производить или на добровольцах, которые хотели поскорее попробовать что-то новое. Таких рабов называли тестировщиками. Если из них кто-то заболевал, то его тщательно исследовали, ну а если и умирал, брали нового.

Таким образом был реализован первый в истории бета-тестинг. Он и сейчас успешно используется в некоторых бесплатных антивирусах (пользователи не догадываются, что они просто бесплатные лабораторные кролики). Этот же принцип успешно используется некоторыми производителями операционных систем. Там пользователи в погоне за новым и новейшим сами устанавливают себе бета версии и (!) даже гордятся этим. Читателю.

Вот так и появились две и сегодня применяемые технологии – общедоступный бета-тестинг, применяемый широко в нашей жизни и Whitelist, успешно применяемый некоторыми антивирусами.

Сказки о безопасности: Наводим порядок в хранилище заклинаний, или технологии iSwift и iChecker

В дальнем-дальнем королевстве существовала Академия магии с известной огромнейшей библиотекой заклинаний. Но каждый раз перед Хранителем библиотеки вставал страшный вопрос: как обеспечить целостность книг? Не дай Бог, какая-то книга будет изменена! И решил он обратиться за помощью к Ректору.

Думал-думал Ректор и решил на каждую книгу наложить заклинание и составить таким образом таблицу, в которой будет имя книги, полка и место ее хранения, а также количество содержащихся в ней гласных и согласных букв, рисунков и страниц.

Читателю. Так Ректор открыл технологию контрольных сумм. В будущем такую же технологию применит в своих антивирусах Лаборатория Касперского. Так появились технологии iSwift и iChecker.

Чуть позже Ректор решил, что подобные проверки книг нужно применять регулярно. В дальнейшем определение подобных контрольных сумм книг выполнялось регулярно, и, если контрольная сумма совпадала с записанной при предыдущей проверке, книга сразу откладывалась в сторону без проверки. Если же не совпадала, то книга подвергалась дополнительной проверке с последующим уточнением контрольной суммы.

Таким образом контроль за книгами была существенно упрощен, и Академия получила дополнительное время для новых исследований.

Читателю. Увы, время, затрачиваемое на проверку файлов, непрерывно растет, и технологии контрольных сумм позволяют существенно упростить и ускорить такую проверку.

Сказки о безопасности: Как рождался BYOD

В дальнем-дальнем королевстве правил король Жадина I. Королевство его, прямо скажем, было небогатое. В первую очередь, потому что разорил всех Жадина налогами. Не понимал он, как это дать людям возможность богатеть, а уж потом брать налоги. Хотел он быть богатым сегодня и сразу. Да не получалось.

Если уж хотите быть богатым и успешным, помните, что само по себе ничего не бывает. Сначала нужно потрудиться! Читателю.

И вот пришла ему в голову идея. Увидел он, как каменотесы на работу шли со своими инструментами. И решил Жадина I, что и воины могут идти на службу со своим оружием и своей амуницией. Да еще и выгода будет в том, что купить это все они смогут в его магазинах. Получается, вдвойне выгодно!

Сказано – сделано! Отныне каждый воин должен был являться в армию со своим оружием и амуницией. Долго ворчал главный военачальник, мол, это будет безобразие, зоопарк, а не армия. Но короля поддержал министр финансов, мол, в государстве денег нет, а так будет чем казну пополнить.

И обозвали они это начинание так – BYOD (Bring Your Own Device)!

Прошел год. Решил король устроить смотр своей армии. Пригласил зарубежных гостей, мол, посмотрите, как здорово я придумал. Учитесь.

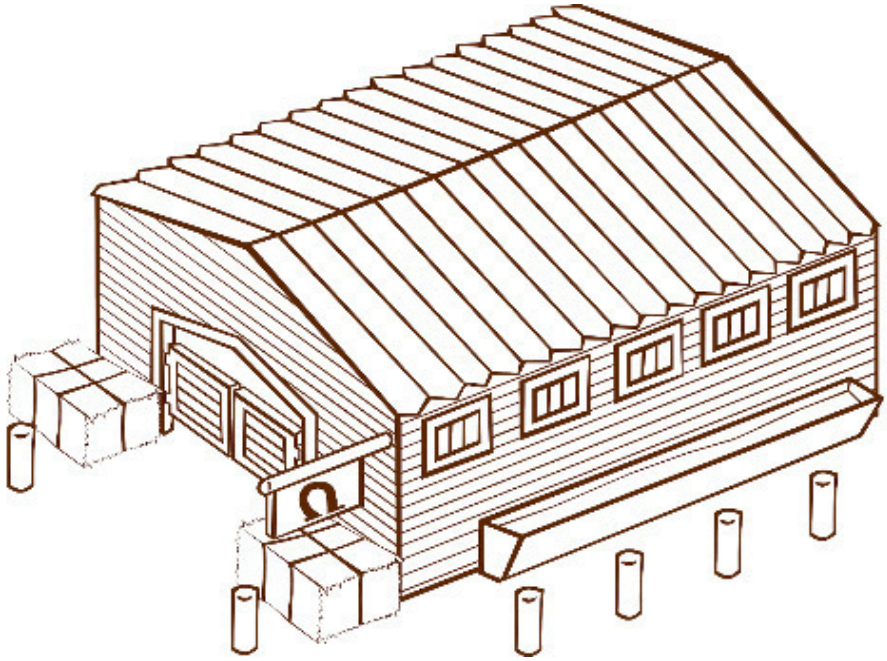
Долго хохотали гости над армией – пришла какая-то банда нищих. Кто в дедовском кожаном колете, а кто в старой-престарой помнящей прадеда кольчуге. Кто с мечом, кто с вилами, кто с косой, кто с топором.

Но еще страшнее выглядела конница.

Вместо племенных жеребцов каждый приехал кто на осле, кто на козле, а кто на верблюде. И начали они расползаться по полю, пугаясь друг друга и вереща на все голоса звериные. Тут-то командующий конницей и был отправлен на плаху, как опозоривший короля перед гостями заморскими.

Хотели, как лучше, а вышло, как всегда. Только усложнили жизнь командирам – кто ж знает, как всем этим зоопарком управлять? Так и в нашем ИТ. Разработают стратегию BYOD, внедрять начнут. А на самом деле – зоопарк с больными и неуправляемыми животными. А где брать для них лекарей и дрессировщиков? Вроде и хороша идея, но результат… Читателю.

Сказки о безопасности: Создание архива эталонного ПО



В дальнем-дальнем лесном королевстве Хольмгард правил король Эрик. Королевство располагалось посреди лесов, и основными товарами в нем были дерево и мед. И дома там были тоже деревянные. Поэтому больше всего в королевстве боялись пожаров.

Читателю. Как ни странно, но и сегодня пожары, затопления и просто выход аппаратуры из строя являются одной из существенных угроз. Как видите, это понимали и в давние времена, а потому создание резервных копий – наше все.

Еще дед короля Эрика издал указ о создании королевского архива. Указ был секретным и разглашению не подлежал. Согласно этому указу все королевские грамоты, указы и основные документы подлежали хранению в королевском архиве, а для работы создавались их копии, заверенные специальной королевской печатью. Документы же из архива (подлинники) выдавались строго по указу короля.

Хранились документы в старой соляной шахте, благо и влажность, и температура в ней были постоянными, и гореть там было нечему.

Читателю. О микроклимате при хранении резервных копий позаботьтесь заранее. А то ни копий, ни подлинников.

В то лето было очень жарко. Пожары в лесах случались часто. И как-то раз загорелся и Хольмгард. Никто не знал, был ли то специальный поджог или просто так случилось. Но сгорело здание королевской библиотеки, в которой, как считали все вокруг и как говорил сам король, хранились все королевские бумаги. Не прошло и пары дней, как вдруг посол соседнего королевства напомнил, что согласно договору с отцом Эрика, соседям отходила часть земель королевства. Это не было правдой, но, как считал соседний король Жадина I, почему бы и нет, ведь договора нет!

Читателю. Еще раз напомню, если у вас все копии зашифрованы вредоносом-шифровальщиком, то кому вы что докажете?

Каково же было удивление посла, когда на приеме Эрик показал ему подлинник документа, в котором ни слова не было о землях.

Читателю. Напоминаю о таком подразделении как конкурентная разведка. Если у вас его нет, то сидите и не высовывайтесь! Репутация создается очень долго, а рушится моментально!

И ушел посол несолоно хлебавши, а репутация короля Жадины так и осталась низкой, что он ни делал.

Читателю. Еще в давние времена появилось такое понятие как архив эталонного программного обеспечения. И сегодня в каждой уважающей себя организации существует архив эталонного ПО, а работают с его копиями.

Сказки о безопасности: Как родилась технология DLP

Было это давным-давно. В дальнем-дальнем королевстве жил да был король. И решил король организовать свою службу доставки указов в дальние провинции. Создал службу курьеров, построил станции для их отдыха. Станционными смотрителями, как правило, назначались бывшие курьеры, что позволяло экономить на их проверке службой безопасности, либо сотрудники этой службы.

Читателю. Уважаемый читатель, вы же прекрасно понимаете, что ни одна служба безопасности не может себе позволить иметь бывших сотрудников. Поэтому в таких службах бывших просто не бывает.

Курьерские сумки опечатывались магическими печатями, вскрыть которые могли только те, кому предназначались соответствующие сообщения.

Но как избежать того, чтобы курьер не увез с собой копию сообщения? Начальник курьерской службы разработал для курьеров специальную форму – без карманов. Чтобы нельзя было что-то в них скрыть.

Король, в свою очередь, решил создать специальное подразделение, сотрудники которого проверяли содержимое курьерской сумки перед опечатыванием и вкладывали туда опись документов.

Так родилась первая цензура.

Читателю. Вам это не напоминает ситуацию с применением учтенного списка флешек? А зря. В принципе ситуация та же. Запрет персональных флешек на работе – существенная часть политики защиты информации.

Ни один курьер не знает куда он поедет, пока не получит сумку. Это позволяет скрыть его маршрут. Везти же что-то помимо сумки – категорически запрещено. За этим должны были смотреть на всех станциях.

Так родился первый учет почты.

Читателю. Ничто не ново под луной. Запомните – все, что пересылается в зашифрованном виде, должно оставаться в копии, а ключи шифрования должны храниться так, чтобы можно было открыть любое шифрованное сообщение в любое время. Любой закрытый документ должен иметь метку, которая позволит его отследить. Использование флешек в большинстве случаев должно быть запрещено, а там, где это разрешено, необходимо контролировать, что именно копировалось с флешки или на нее.

Вот так и появились первые DLP-системы.

Сказки о безопасности: Охрана периметра

На дальней дороге, ведущей в замок, встретились Дракон и Рыцарь, которому нужно было проехать в замок.

– Дракон, ты чего тут сидишь?

– Дорогу охраняю! В замок!

– От кого?

– От всех!

– А если они полем пойдут?

– Поле я не охраняю.

– То есть по полю я могу проехать свободно?

– Нет! Там забор!

– А как же мне попасть в замок?

– Никак! Нужно знать пароль.

Долго сидели спорили. Пока в конце концов Рыцарь не спросил, а подземный ход есть?

– Конечно, – ответил Дракон, – Сколько угодно.

– А по ним как? Можно?

– Свободно! Я ж только периметр охраняю.

Читателю. Вам это ничего не напоминает? Охраняем периметр сети, а с мобильных устройств войти в сеть можно? Да хоть пешком! Понятие периметра размыто и охрана периметра сегодня явно недостаточна.

– Погоди, а я проеду в подземный ход?

– Конечно, у нас подземные ходы (каналы) с хорошей пропускной способностью.

– Так, а зачем ты тут?

– Поставили и забыли, вот и сижу!

– И что, никто ни разу через подземный ход не ходил в замок?

– Да что ты! Это здесь никто не ходит, а там как на проспекте!

Читателю. Вот так и в жизни. Периметр охраняем, а с мобильных устройств заходит в сеть, кто хочет, лишь бы пароль знал.

Попрощался Рыцарь с Драконом и уже через несколько минут был в Замке.

Сказки о безопасности: Как появился DDoS

В дальнем государстве правил король. Народ дал ему прозвище Эрик Справедливый, потому что самые сложные случаи разбирал он в своем суде справедливо, и были перед тем судом равны все – и вельможи, и простолюдины. Так продолжалось много лет. Но однажды собрались наиболее влиятельные вельможи и решили, что так нельзя. Мол, как это простой крестьянин и герцог равны перед судом?

И решили они заблокировать работу королевского суда, чтобы король сам заявил, что не может справиться с нагрузкой.

Читателю. Самый простой способ заблокировать ваш сайт – сделать так, чтобы он не успевал обслуживать запросы пользователей. Если это достигается с помощью специально организованного одновременного обращения к сайту большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, поддерживаемый не очень производительным сервером. Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

Как решили заблокировать суд? Посылкой огромного числа запросов, в том числе правильных и неправильных.

Читателю. Не правда ли, стандартная DDoS-атака?

Огромное количество жалоб и заявлений посыпалось в королевский суд. Все служащие были вынуждены разбирать завалы писем, пока кто-то из них не обратил внимание на то, что слишком много запросов идут типовых, похожих друг на друга, да еще и с одних и тех же почтовых станций.

Читателю. Так появился первый в истории спам-фильтр.

Письма с этих станций просто перестали обслуживать, и поток тут же иссяк. Однако король поручил разобраться, почему письма схожи между собой. Оказалось, все они были написаны как под диктовку да к тому же одним и тем же почерком. На станции были направлены секретные агенты, которые быстро вычислили писавших. Все нити вели к заговору вельмож, который и был ликвидирован в кратчайшие сроки, а королевский суд успешно продолжил свою работу.

Читателю. Так впервые в истории закончилось успешно дело о спам-рассылке и попытке блокирования королевского суда. Первая DDoS-атака в истории королевства была успешно отражена.

Сказки о безопасности: Магические существа, или как защититься от вредоносов-шифровальщиков

Два королевства граничили друг с другом. В одном правил Эрик Справедливый, а в другом – Эдвард Жадина, которого чаще всего называли Жадина I. И все было бы нормально, да вот только поселился в темном лесу маг. Да уродился тот маг жадиной похлеще Эдварда. За копейку готов был удавиться.

Надумал маг сделать так, чтобы королевства ему дань платили. И вот что придумал. Создал он волшебных существ, да таких маленьких, что не видны они были невооруженным глазом, а питались те существа чернилами с пергаментов. И решил маг, что если выпустить их где-то недалеко от архива, то они уничтожат все пергаменты в архиве, а чтобы восстановить написанное, придется королю заплатить.

Читателю. Не правда ли, похоже на поведение нынешних вредоносов-шифровальщиков? Зашифровать все документы и просить выкуп.

Сказано – сделано. Попробовал маг такое на своих рукописях – получилось. Как уничтожить, так и восстановить.

Послал он гонца с такими существами в соседнее королевство – все вышло, заплатили. Тогда решил он объявить об этом вслух, что, мол, есть такая напасть.

Дошло это до Эрика Справедливого. Он и ранее создавал резервные копии, да тут задумался. И вот что сделал. Отныне создавались копии в одной пещере, в соседней накапливались оригиналы для перевозки в основной архив, а тот хранился в дальней пещере – отвозили туда оригиналы дважды в неделю в сопровождении вооруженной охраны.

Узнал об этом Жадина I и решил сделать то же самое у себя. Но вот только он же жадина, поэтому решил сэкономить. Основной архив он просто разместил в том же здании, но в другой комнате.

Читателю. На самом деле мы имеем две реализации резервного копирования: на дисковую стойку в том же здании (Жадина) и на периодически подключаемую, хранимую в удаленном хранилище (Эрик Справедливый). Первый способ существенно дешевле, но в случае заражения вредоносом-шифровальщиком заражен будет и основной носитель информации, и резервный. Во втором же случае основной накопитель будет заражен, но резервное хранилище останется целым.

И настало время, когда попытались атаковать сразу оба королевства. Архив Жадины I был уничтожен полностью, а архив королевства Эрика Справедливого уцелел, заражены были копии и те документы, которые не успели перевезти. Но их было совсем мало. Таким образом, основная часть документов короля Эрика уцелела.

Читателю. Увы, никакой антивирус не может служить гарантией от заражения вирусами-шифровальщиками. Только резервное копирование на отключаемый внешний носитель может вас защитить.

Короли объединили свои войска и воспользовались помощью магов. Злой волшебник был наказан, но не убит – сбежал в последний момент.

После этого он решил, что слишком опасно самому и заражать жертв, и получать деньги, поэтому сосредоточился исключительно на создании вредоносных магических существ, которых уже просто продавал злодеям за деньги.

Читателю. И сегодня среди злоумышленников существует разделение труда: одни разрабатывают конструкторы вредоносов-шифровальщиков, другие их используют, а третьи собирают дань. Как правило, арестовывают только третьих.

Сказки о безопасности: Как Эрик Справедливый с напастью справился, или Облачная защита от DDoS-атак

После бунта вельмож снова заработал королевский суд, и король Эрик Справедливый решил, что с возникшей было проблемой покончено. Но не тут-то было. Пришла беда, откуда ее уже не ждали. Собрались мятежники с силами и начали слать еще больше писем, еще больше непонятных запросов. Снова стала захлебываться королевская почтовая служба.

Читателю. Не стоит думать, что если один раз удалось отразить DDoS-атаку, то на этом все и закончится. Атаки будут повторяться вновь и вновь, и каждая последующая может быть изощреннее предыдущей.

Но не бывает на свете безвыходных ситуаций. Узнал король, что в соседнем королевстве Академия магии организовала службу защиты от подобных атак, направив в нее специально обученных магов. Послал Эрик Справедливый туда своего гонца разузнать, что и как. Не прошло и трех дней, как вернулся гонец с письмом-предложением – бралась специальная служба Академии магии решить проблему короля, организовав у себя отбор обращений в королевский суд.

Подумал король, взвесил все «за» и «против» и согласился – надо же как-то выходить из положения. С этой поры обращения шли не напрямую в королевскую почту и к королю Эрику, а на специальную фильтровальную станцию. Там отсеивалось все ненужное, а все нужное направлялось Эрику с гонцами. Поскольку делом занялись не обычные почтовые служащие, а специально обученные маги, да и было их больше, обрабатывали поток они значительно скорее.

Читателю. Если поток обращений к вашему ресурсу зашкаливает, есть смысл воспользоваться облачным фильтром, который, имея возможность использовать нужное количество серверов и необходимую полосу пропускания канала, обработает входной поток существенно быстрее и таким образом защитит вас от DDoS-атак. Соответствующие технологии получили название Security as a Service (безопасность как сервис).

Суд у короля заработал исправно. А министр финансов даже сумел сэкономить на количестве гонцов и разборщиков писем-обращений.

Читателю. Используя Security as a Service вы тоже сможете сэкономить как на ширине канала, обеспечивающего доступ к вашим ресурсам, так и на мощности серверов для фильтрации входного потока. Помните об этом!

Сказки по безопасности: Как король Эрик опыт Жадины I переосмыслил, или от BYOD к CYOD!

После провала эксперимента короля Жадины I, когда он потребовал от своих воинов со своим оружием и амуницией на службу являться, задумались другие короли – нельзя ли как поумнее придумать: оно вроде как экономия, да, получилось, не та экономия. Решил король Эрик Справедливый, что иначе нужно все делать.

Позвал он своего канцлера и министра финансов и распорядился дать работникам и служащим возможность выбирать, что им надобно для работы и несения службы, но не просто так, а из предварительно составленного перечня, дабы потом смеху из затеи не вышло. То есть сначала комиссия из людей, знающих перечень составляет, а уж потом работник из него выбирает то, что ему сподручнее. И не сам за то платит, а из казны средства выделяются. Получается, и работнику хорошо, и делу на пользу (не сошлешься теперь, что работа стоит, потому что хорошего инструмента не дали – сам выбирал ведь). Мало того, пообещали работникам, что через некоторый срок выбранное ими для работы отдадут им в собственность.

Читателю. Представьте, что ваша компания с учетом мнения ИТ- и ИБ-специалистов отберет смартфоны и планшеты и предложит вам выбрать себе наиболее подходящий гаджет, пообещав, что через некоторый срок он станет вашим. Как вы к этому отнесетесь? А если это не гаджет, а автомобиль?

Прошло немного времени, и увидел король, что и кони стали выглядеть лучше, и инструменты всегда вычищены и в исправном состоянии, и работа идет веселее. А министр финансов доложил ему, что на всякого рода ремонты денег уходить стало куда меньше, а в казне, наоборот, их прибавилось. Богатеть королевство стало.

Читателю. Пользу перехода от BYOD к CYOD (Choose Your Own Device, «Выбери свое собственное устройство») уже поняли многие компании. В результате упрощаются администрирование и защита используемых для работы мобильных устройств, а финансовые затраты компании по сравнению с BYOD даже снижаются.

Единственными, кто не радовался изменениям в королевстве, были ремонтные службы. Но их мнение уже никого не интересовало.

Сказки о безопасности: Как король принца образумил, или Не знаешь – не трогай!

В дальней-дальней стране жил-был любопытный принц. Все ему было интересно, и решил он начать собирать удивительные и волшебные вещи. Да вот беда – не хотел учиться, как обращаться с теми вещами, мол, и без учения разберется. Уж и так его увещевали и эдак, ан нет – не нужно ему. Сам ученый, и делу конец.

Читателю. Вам не кажется, что это весьма похоже на поведение некоторых хвастливых администраторов (пользователей), которые уверены, что документацию читают только бездари? Вы с такими не сталкивались?

И вот однажды попалась принцу в руки небольшая коробочка, на которой было написано «Открывать только в случае смертельной опасности и только в присутствии друга!»

Принц был не только любопытен, но и самонадеян: «Мало ли что написано! Открою!» Открыл и… окаменел! На его счастье недалеко находился садовник. Подхватил он выпавшую из рук принца коробочку и побежал к королю.

Читателю. Хорошо, если рядом оказывается кто-то, готовый помочь в непростой ситуации. А ведь бывает, что и нет никого.

Выслушал король садовника, осмотрел коробочку. На дне ее обнаружил надпись: «Пусть друг вложит коробочку тебе в руки, и ты оживешь!»

Король был умным отцом и сказал, чтобы принца никто не трогал неделю. Так в саду под дождем и ветром принц неделю и простоял. И только после вложили принцу коробочку в руки, и он ожил.

Читателю. Учитесь, прежде чем что-то делать! Читайте документацию, тренируйтесь, а уж потом внедряйте то или иное ПО или оборудование. Помните, что устранить проблемы, возникшие в результате неправильного применения ПО и оборудования, бывает гораздо труднее.

Сказки о безопасности: Как король дворец строил, или О пользе сертификатов

Задумал король дворец строить – что за столица без дворца? Решил пригласить архитекторов и сам с ними побеседовать.

Читателю. Если вы подбираете персонал для важного дела, проводите собеседование с ними сами. Так вы скорее определите, подходят они вам или нет.

Странным, однако, было то, что король сразу отсеивал выпускников местных и зарубежных университетов, всевозможных мастерских и курсов. Всех, у кого были дипломы и сертификаты. Сколько ни поясняли ему, что эти люди образованы и доказали свои знания и умения, король был непреклонен.

Выбрал король себе архитекторов. Не самых лучших, не самых худших, но выбрал.

Приехал к королю в гости Верховный Маг и спрашивает: «Король, а почему ты всех сертифицированных да дипломированных специалистов разогнал?»

Ответил король: «Не поверишь, завидую я им. В детстве была у меня учительница – старая, злая жаба. Учила она меня читать. Чуть что, розгами драла! Так и не выучила толком, да вот с тех пор я завидую тем, кто выучился. Потому и не беру к себе сертифицированных да дипломированных. Робею…»

Читателю. Надеюсь, вы-то хорошо учились – не как тот король. И понимаете, что наличие сертификатов у специалиста говорит о том, что он работает над собой. Имеет и знания передовых технологий, и желание учиться далее. Хотя, безусловно, курсы бывают разные, да и сертификаты тоже.

Сказки о безопасности: Как король Эрик с нечистью боролся, или О пользе учения

– Образованию нужно не в реанимацию, а на кладбище!

– Это будет большое неупокоенное кладбище – и тогда специалистам по безопасности придется стать еще и некромантами.

Никто не знает, откуда взялась и как стала плодиться эта новая зараза в королевстве Эрика Справедливого. Отголоски великих магических войн, бушевавших на земле, давно утихли. Полагать, как в старь, что это-де мятежные маги продолжают выводить в мир нечисть, стало попросту невозможно. До чего дошло – ведь уже не маги, а любой, у кого есть кошелек с несколькими монетами, может сам создать зомби или выпустить в свет новую заразу. Не нужно магом становиться, проще заплатить за магический конструктор – и твори-плоди новые сущности.

Читателю. Вам это не напоминает сегодняшнюю ситуацию с распространением вредоносного кода? Для его создания уже не нужно разбираться в тонкостях программирования – можно купить или взять в аренду конструктор, причем даже с технической поддержкой. Результат – огромное количество вредоносов.

Множатся ряды зомби, вмиг охватывают города губительные эпидемии.

Читателю. От появления новой заразы до первого заражения, по данным антивирусной компании Trend Micro, в среднем проходит всего 82 секунды .

А коли началась эпидемия, уже не помогают, как раньше, проверенные огненные валы – сама почва и воздух, похоже, становятся заразными. Не выручают ни стражники в городских воротах, ни посты с ратниками на перекрестках и переправах… Зараза мутирует, приспосабливается, и стоит ей угнездиться в одном-единственном доме, как скоро целые кварталы ею кишат.

Читателю. Если в вашей сети произошло заражение, проверять, скорее всего, придется все ПК – и те, в которых зараза уже себя проявила, и те, что ведут себя как «чистые». Имейте в виду, что еще недавно помогавшие файерволы могут оказаться бессильными, ведь сегодня ноутбуки и мобильные устройства по нескольку раз в день пересекают границу их действия.

Усилил король Эрик корпус Магов-Защитников, многие школы при коллегии Магов начали их готовить. Да вот проблема. Учить-то они учат, а побороть заразу не получается.

Думали-думали в чем причина, и вот к чему пришли. Проблема в том, что нечисть все время мутирует, а учат Магов-Защитников одному и тому же. И большинство из них после окончания школы учатся исключительно на своих ошибках – учебники мало кто читает, а еще меньше кто их понимает.

И решили король Эрик с Верховным Магом исправлять положение. Эрик Справедливый издал указ о том, что Маги-Защитники, выпускающиеся из школы в четный год, отныне и на будущее будут проходить дополнительное обучение каждый четный год, а выпускающиеся в нечетный год – в нечетный. И кто не учится, тот не сможет остаться в корпусе Магов-Защитников. И пошло дело на лад – пошла на убыль зараза.

Читателю. Повышение квалификации ИБ- и ИТ-персонала – проблема огромная. И решать ее нужно не только в сказках. Любая профессия требует постоянного обучения, но в быстро меняющейся сфере ИТ и ИБ – это актуально как нигде.

Сказки о безопасности: Как король Эрик купца и его бывшего приказчика рассудил

В королевстве Эрика Справедливого высшим судом был королевский суд, управляемый самим Эриком и назначаемыми им судьями.

Однажды на королевский суд пришел купец Эдвард со своим бывшим приказчиком Нортом, который уволился и перешел к конкуренту. Да не просто перешел, а переманил за собой часть покупателей, с которыми имел дело на прежней работе, чем нанес Эдварду немалый ущерб. Хорошо зная своих клиентов и пользуясь их доверием, Норт убедил их, что у его нового хозяина товар лучше. И перестали они покупать у Эдварда.

Читателю. Типичная история, не правда ли? Увольняясь с работы, менеджер по продажам уносит с собой и базу клиентов. Более того, без «своих» клиентов на новое место его, скорее всего, и не взяли бы.

Выслушал король купца и спросил, говорил ли тот своему приказчику, что поступать так нельзя, и заключал ли с ним об этом соглашение, закрепленное на бумаге подписями обеих сторон. И есть ли у купца перечень того, о чем его работникам рассказывать другим запрещается? И ознакомлены ли с этим перечнем работники?

Читателю. Надеюсь, в вашей компании все в порядке – и перечень конфиденциальной информации есть, и сотрудники с ним ознакомлены, что подтверждено их подписями.

– Нет, – ответил купец, – Никогда у нас не было таких бумаг, ведь и так понятно, что поступать так нельзя!

– Погоди, то есть ты об этом не говорил и бумагу вы не подписывали?

– Нет! Мы всегда доверяли друг другу!

– В таком случае сам виноват, – рассудил король Эрик.

Король принял справедливое решение, и купцу еще штраф пришлось заплатить за собственную беспечность. А бывший его приказчик ушел домой довольный.

Читателю. Помните, даже если вы с помощью технических или иных средств выявили действия, которые заведомо наносят компании ущерб, а организационного документа, подтверждающего, что подобные действия считаются нарушением, у вас нет, то предъявить претензии сотруднику вы не вправе. Технические средства контроля действий сотрудников должны быть подкреплены организационными мерами. Но справедливо и обратное – организационные меры защиты конфиденциальной информации следует дополнять техническими средствами контроля. Они помогут снизить вероятность нежелательных инцидентов.

Сказки о безопасности: Как купцы голема продавали, или Зачем нужна документация

В королевстве Эрика Справедливого все, от мала до велика, знали, что король собирает диковинки. Разные магические и не магические диковинные вещи.

Как-то раз приехали купцы из-за моря. Привезли для короля магического голема, который, по их словам, мог бы охранять королевский замок.

Решили показать королю, что же на самом деле умеет голем. Выехали купцы на огромное поле перед королевским замком показать товар лицом.

Один из купцов включил голема. Страшное железное чудовище с огромными мечами и горящими красными глазами поднялось над полем и вдруг… бросилось на купцов. Долго гонялся голем за купцами. Все поле оглашалось криками.

Долго смеялась свита короля над незадачливыми купцами, пока король что-то не выкрикнул с башни, и голем встал и выключился.

Купцы не могли понять, что же кричал король. А тот просто посоветовал незадачливым купцам в следующий раз, когда они будут везти диковинки, особенно боевые, предварительно читать документацию к ним.

Читателю. А вы всегда знакомитесь с документацией, прежде чем устанавливать соответствующее программное (аппаратное) обеспечение? И не забывайте менять установленные по умолчанию логины (пароли), с помощью которых вы сможете сменить соответствующие настройки. Потребуйте того же от ваших администраторов.

Сказки о безопасности: Как король Эрик и с заразой справился, и казну от чрезмерных расходов уберег

В королевство Эрика Справедливого пришла беда. Начался падеж скота, да и посевы на полях поразила неизвестная болезнь. До эпидемии дело еще не дошло, но беспокойство в королевстве возникло нешуточное.

Призвал Эрик на помощь Академию Магии, но не смогли ее маги справиться с напастью. Тогда распорядился Эрика доставить зараженных животных и больные растения в разные магические лаборатории других королевств, с которыми Академия связь поддерживала.

Читателю. Если вы заподозрили, что столкнулись с вредоносным кодом, но не уверены в этом, проверьте подозрительные файлы не одним, а несколькими антивирусными решениями, для чего оборудуйте в департаменте ИБ специальный ПК.

Сложной оказалась задача, но две лаборатории все же откликнулись со своими предложениями, как справиться с нависшей угрозой. Правда, оказались они не равноценными: одно – очень хорошее, но очень дорогое; другое – в целом не такое эффективное, хотя со своими плюсами, но зато и не такое для казны обременительное.

Призадумались советники короля Эрика – как же быть? Тут один из советников и говорит:

– А давайте подумаем, как зараза распространяется? Во-первых – через сухопутную или морскую границу. Во-вторых, если она уже проникла в чье-то хозяйство, то в город ее можно занести через городские ворота, в другие хозяйства – через ярмарку, где скот продают и все необходимое для ухода за посевами. Здесь скупиться – себе дороже, поэтому нужно лучшее решение использовать.

– Так ведь и хозяйства нельзя без защиты оставить, – возразил Эрик.

– А мы и не оставим, – пояснил советник. – Но для них и второе решение подойдет. Оно ведь тоже неплохое, и у него свои преимущества имеются. И ежели зараза через первый кордон просочится, глядишь, второй как раз и справится – два-то разных решения, возможно, лучше сработают, чем любое одно!

Так и сделали. Меры, которые предложила первая магическая лаборатория, распространили на пограничные пункты, городские ворота и ярмарки. А в замках и хозяйствах подданных короля Эрика обошлись тем предложением, что подешевле. И не прогадали!

Читателю. По такому же принципу строится двухуровневая антивирусная защита: шлюзы, почта, периметр сети защищаются одним антивирусом, а сервера и рабочие станции другим. Управлять таким решением сложнее, но оно позволяет обеспечить необходимый уровень защиты ресурсов предприятия при приемлемых затратах.

Сказки о безопасности: Как в королевстве телефонную связь делали, или помните о паролях по умолчанию

С одной стороны, королевство Эрика Справедливого граничило с королевством Жадины I, а с другой, было окружено непроходимыми горами с обрывистыми скалами и глубокими пещерами.

Как-то раз увидели пограничники, что с гор едет к ним посольство. Оказалось, что это посольство гномов.

Непонятно, что заставило подгорный народ выбраться на поверхность и ехать к королю. Но гораздо интереснее было то, что привезли они в дар. А привезли они – телефон! Да не просто линию оборудовали между двумя королевствами, а линию с шифрованными переговорами. Установили они в кабинете короля два телефона. Один – для переговоров с подгорным королем, а второй – для связи с военным министром, премьер-министром и другими абонентами. Настроили телефоны, обучили подданных Эрика, вручили документацию, наказали ее прочесть, изучить и уехали.

Все бы хорошо, но донесла разведка Эрику, что все его переговоры быстро становятся известны агентам Жадины I.

Вызвал король гномов. Что он им сказал – неизвестно, но работали они как проклятые три дня и три ночи.

На четвертый день пришли они к Эрику и попросили позвать местных техников-связистов.

– Вы документацию читали? – спросил главный гном.

– Конечно!

– Врете! Что написано на первой и на последней странице?

Задумались местные связисты.

– Не помним, – честно ответил кто-то.

– Вот-вот! А на первой странице написано – смените пароль по умолчанию!!! Вы это сделали? Нет!

– А на последней написано. «Дочитали? Молодцы! А пароль сменили?!!»

Эрик попросил прощения у гномов и повелел выпороть связистов. А через месяц попросил приехать гномов и принять зачеты. А кто не сдаст – выпороть снова и потом провинившийся сам поедет в горы сдавать зачет!

Я надеюсь, что ваши ИТ- и ИБ-специалисты читают документацию и меняют пароли по умолчанию. Если нет – берите пример с Эрика, уж точно не забудут! Читателю.

Сказки о безопасности: Как король Эрик главного стражника выбирал

В королевстве Эрика Справедливого пришло время искать нового начальника стражи королевского замка – прежний свое отслужил, да и трудновато ему стало с новыми угрозами справляться.

Дело серьезное, а потому с каждым претендентом король решил беседовать лично. Кандидатов было не много, не мало, но вот очередь дошла до Рагнера Осторожного.

Рагнер полностью оправдывал свое прозвище. Ни одного ответа он не давал прежде, чем тщательно все не обдумает. Казалось, он взвешивает не то что каждое слово – каждый жест, каждый вздох.

Поинтересовался король у Рагнера, с чего он начнет, если будет назначен начальником стражи королевского замка. Рагнер подумал и ответил, что главное, по его мнению, заключается в том, чтобы прописать на бумаге, что и как в замке можно делать и чего нельзя, а потом затвердить ее королевской печатью и заставить всех стражников и тех, кто бывает в замке, под этой бумагой расписаться – мол, ознакомлены и обязуются исполнять. Всего и делов-то! И затрат больших из казны не потребуется – все грамотные, а потому пусть читают внимательно. А если кто не так что сделает и опасность какую прозевает, ему и отвечать за последствия – бумагу ведь подписал.

У вас в компании так не бывает? Сегодня между делом вы инструкцию подписали, наспех проглядев, а назавтра уже забыли, о чем в ней говорится. И так до следующего раза, если, конечно, раньше гром не грянет, и вы не окажетесь виновными в том, что в чем-то не соблюли ту инструкцию. Читателю.

Усмехнулся король – получается, что бы в замке ни случилось, Рагнер в этом уж не виноват вроде: бумагу король утвердил, а кто ее подписал и не исполнил – с того и спрос за все. И велел Эрик Справедливый дать Рагнеру Осторожному бумагу подписать, что ближе версты к замку подходить не будет, а если невзначай нарушит условие и попадется, то выпорют его на королевской конюшне – сам виноват!

Не спешите подписывать инструкции, не ознакомившись с ними внимательно. Попросите, чтобы вам обязательно оставили копию, и в сомнительных ситуациях убедитесь, что не нарушаете те или иные положения принятых в компании и подписанных вами документов. Вместе с тем, руководителям служб предприятия, в том числе службы ИБ, вряд ли стоит полагаться только на то, что опасения понести ответственность гарантируют отсутствие ошибок в действиях сотрудников. Убедиться в том, что последние правильно понимают суть подписанных ими документов и помнят их главные положения по прошествии времени, – прямая обязанность ответственных руководителей. Это позволит избежать неприятностей и для сотрудников, и для их руководителей, и для компании в целом. Читателю.

Сказки о безопасности. Эльфы и стеганография

После появления в стране Эрика Справедливого гномов с их телефоном прошло не так много времени. И вот к королю приехала новая делегация – эльфы. Казалось, что ничто не способно удивить ни короля, ни горожан столицы. Но эльфы?! Народ, который отгородился от людей, не принимал у себя делегатов от других королей и никуда не ездил сам.

Однако удивляться было чему еще впереди. После официального визита к королю состоялся еще и малый, тайный прием, на котором эльфы поведали тайну своего народа.

Оказывается, эльфы различали гораздо больше цветовых оттенков, чем люди, а, следовательно, использовали гораздо больше красок. И тайна состояла в том, что посредством различных оттенков они умудрялись зашифровывать в рисованных картинах целые послания. Так, обычный зеленый цвет у них имел более 32 оттенков, впрочем, как и красный и другие цвета. Таким образом, рисуя картины, они могли записывать в них целые послания, не нарушая при этом цветовую гамму.

Так началась дружба и шифрованная переписка с эльфами.

Так родилась стеганография

Помните, что, если кто-то в вашей организации очень любит отсылать наружу картинки, это могут быть и не совсем безобидные картинки. Обратите на это внимание. Может наружу отсылают ваши корпоративные секреты, а вы об этом не подозреваете? А?

Сказки о безопасности: Гномы и ИБ-кадры

После внедрения гномьего телефона и подсказки эльфов об асимметричном шифровании королевство Эрика столкнулось с другой проблемой – где взять специалистов? Организовать срочно курсы? Пригласить гномов и эльфов обучать? Но специалистов требуется много…

Решено было сделать иначе – силами гномов и эльфов подготовить преподавателей, а уж дальше учить самим. Но обнаружилась другая проблема. Если на курсы преподавателей еще смогли найти людей, которые хорошо знали бы математику, то вот дальше…

Так родилась идея специализированных школ, в которых математику изучали бы глубже, чем в обычных. И вместе с университетом появились специализированные школы.

На самом деле вывод довольно прост. Если вы хотите иметь сильное государство и всерьез заниматься безопасностью, вам потребуются кадры, которые нужно готовить заранее. На пустом месте ни криптографы, ни криптоаналитики, ни просто математики не рождаются.

На становление системы подобного образования королевству потребовалось много лет и много средств. Но зато потом уже к ним приезжали учиться из-за рубежа. И платили за это золотом. А специалисты этого университета очень высоко ценились во всем мире.

Следует признать, что подготовка специалистов в области безопасности должна начинаться со школы. И чем умнее и талантливее учителя, чем выше престиж работы Чем лучше учителя, тем лучше будут подготовлены кадры. Мораль проста. Хотите обеспечить безопасность – учитесь! Учитесь и учите, иначе так и будете использовать неизвестные продукты и технологии, в которые ваши конкуренты вполне смогут разместить всевозможные закладки. А вы об этом и знать-то не будете.

Сказки о безопасности: Королевский мусор как источник информации

Королевства Жадины I и Эрика Справедливого всегда находились в состоянии вражды. Шпионили обе стороны. Информацию добывали кто как мог. Но шпионы Эрика Справедливого отличились. Они умудрились принести информацию практически из дворца Жадины I. На естественный вопрос лорда-канцлера, как же это возможно, ведь во дворце у нас нет агентов, руководитель тайной канцелярии, хитро улыбнувшись, заметил, что агенты во дворце стоят дорого, знают мало. А потому он решил внедрить своих агентов в команду мусорщиков, обслуживающих канцелярию Жадины I.

А так как Жадина I вполне оправдывал свое прозвище и экономил на всем, то черновики бумаг записывали на обратной стороне уже использованных документов, а потом не сжигали в специально выделенной печи, как это делали во дворце Эрика Справедливого, а просто собирали для повторной переработки, чтобы сэкономить на производстве бумаги. Вот эти черновики и анализировались специальной командой мусорщиков.

А у вас бумажный мусор собирается в специальных урнах на охраняемой территории? Вы предварительно его измельчаете в специальных аппаратах? А потом уничтожаете в специально отведенных местах в присутствии специальной комиссии? Или вы просто выбрасываете его, чтобы злоумышленникам было легче его анализировать?

Сказки о безопасности: Самое слабое звено королевства

В королевстве Жадины I экономили буквально на всем. Расходы на армию поддерживались на минимальном уровне. Денег едва хватало на еду и жалование. О ремонте крепостей никто даже не заикался. Но проблемой были расплодившиеся разбойничьи шайки. Сколько ни ловили их да не вешали разбойников, голодные крестьяне все чаще и чаще от безутешной доли шли разбойничать.

В крепости Грим, стоявшей у дальней границы, вдалеке от столицы, командовал барон Арн. И все было бы хорошо, да барон подворовывал и те небольшие средства, которые выделялись на крепость. В результате в крепости была грозная стена, башни с толстыми воротами и… огромная дыра в стене с тыльной стороны. Барон считал, что с той стороны подобраться нельзя, так как стояла крепость на скале и, на его взгляд, забраться в нее со стороны дыры было невозможно.

В ту ненастную ночь, казалось, само небо разгневалось на гарнизон крепости. Лил сильный холодный дождь. Небо прорезали огромные молнии. Да к тому же выл сильный ветер. Казалось, что в такую погоду нужно просто сидеть по домам да пить подогретое пиво или горячий грог.

Однако так казалось не всем. В эту ночь большая шайка разбойников решила штурмом взять крепость, куда как раз приехал сборщик налогов этой провинции с небольшим отрядом стражи.

Разбойники поднялись по скале и атаковали крепость как раз со стороны дыры. Крепость пала, а королевский обоз был разграблен.

Помните, что вся ваша безопасность равна безопасности самого слабого звена. В данном случае самое слабое звено в обороне – дыра в стене. И, как видите, сколько не вешай замков на ворота, а дыра в заборе и… крепость пала! Сегодня самое слабое звено – люди. Учите их! Иначе будет поздно!

Сказки о безопасности: Королевские пентестеры

После того как разбойники ограбили крепость и забрали налоги целой области в королевстве Жадины I, король Эрик Справедливый учредил в военном министерстве инспекционный департамент. Данный департамент должен был заниматься инспектированием крепостей и гарнизонов, проверкой боеготовности гарнизонов и уровня знаний командиров.

В состав департамента входило особо секретное подразделение, которое занималось проверкой боеготовности, в том числе путем несанкционированного проникновения на территорию военных городков, лагерей и крепостей. Так появилось первое подразделение пентестеров.

Тестирование на проникновение (жарг. Пентест) – метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу целевой системы, либо полный отказ в обслуживании. Анализ ведется с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. Результатом работы является отчет, содержащий в себе все найденные уязвимости системы безопасности, а также может содержать рекомендации по их устранению. Цель испытаний на проникновение – оценить его возможность осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки. Испытание на проникновение является частью аудита безопасности.

Королевские пентестеры занялись проверка готовности к возможному проникновению врага. Но после проведения нескольких подобных проверок оказалось, что тестирование проникновением это хорошо, однако это не дает реальной картины безопасности. Как быть? Тогда с целью углубленной проверки в инспекционном департаменте было создано подразделение аудита, которое, в свою очередь, проверяло соответствие выполнения приказов министерства и устранение ранее найденных недостатков. По итогам аудита составлялся отчет. Если обнаруживались ошибки, то выделялось время для их устранения. Если же в срок недостатки не устранялись снова, то соответствующий руководитель уходил с понижением, а в случае особо выраженных недостатков – просто увольнялся без выходного пособия и пенсии.

Да, строго, да страшно, но что важнее? Быть добреньким или отвечать за безопасность и жизнь своих подчиненных? По-моему, ответ очевиден. Не можешь – не работай! То же самое касается и вас, господа безопасники. Не забудьте, что вы должны регулярно проверять безопасность вашей сети. Ведь отвечаете за нее вы, не так ли?

Сказки о безопасности: Свобода как оборотная сторона безопасности и порядка

После катастрофы со строительством крепости иностранными фортификаторами Жадина I задумался. На возведение новой крепости денег нет. Своих специалистов нет. Как быть?

Задал он этот вопрос своим министрам. Думали они целую неделю, как вдруг один из министров сказал, что слышал мол – есть команда, которая позиционирует себя как «Свободная команда специалистов». Причем вся прелесть состоит в том, что чертежи они дают бесплатно, а строить вы будете сами. То есть вы сэкономите на архитекторах и патентных отчислениях. Так дешевле! На естественный вопрос, а зачем это самой команде, министр ответил, что эта команда проповедует свободу творчества и состоит из бунтарей, которые считают, что военные фортификаторы обдирают клиентов.

Вам это ничего не напоминает? Например, попытку внедрения свободного ПО? У нас все дешево, налетай, бери! Только помните, что если вы не платите – вы товар!

Решил Жадина I заключить договор с такой командой. Принесли ему чертежи, посмотрели, вроде как все хорошо. Решили строить. Долго ли, коротко ли продолжалось строительство. Построили. Пришел военный министр и просто онемел. Да только совсем не от восторга.

Батареи на бастионах смотрят не в ту сторону. Ворота в крепости направлены в сторону обрыва… Стены из легкого пористого кирпича… И на всех стенах реклама ближайших стриптиз-баров!

Рявкнул министр, мол, что за ерунду вы натворили?

В ответ – все как на чертеже. Его наши лучшие фортификаторы проверяли, ну а то что ворота не в ту сторону, или бастион не такой – так мы тут ни причем. Сообщество проверяло. А кто конкретно? Все! Кто отвечает? А никто! А реклама? Так жрать нам нужно? Да и дома нас ждут. Бесплатно работать-то нельзя!

Плюнул министр и решил, что уволится к чертовой бабушке, лишь бы на такое художество не смотреть. Ответ, мол, зато бесплатно, его явно не устроил.

Нельзя путать свободное и бесплатное ПО с безопасным. Хотите безопасное – покупайте! Хотите бесплатно, привыкайте что вы товар и не вы, а на вас будут зарабатывать. Привыкайте!

Сказки о безопасности: Невосстановимое стирание

В королевствах Жадины I и Эрика Справедливого для особо важных королевских архивов использовался пергамент. Несмотря на то что бумага давно была в ходу, это была, во-первых, дань традиции, а во-вторых, тексты на пергаменте куда как дольше хранились. Одна беда – пергамент в производстве был дорог. Потому в королевстве Жадины I много раз использованный пергамент, удалив кое-как тексты, просто продавали, чтобы сэкономить деньги.

Аналогично они поступали с бумажными архивами, не уничтожая их, а просто сдавая на макулатуру.

Читателю. Не правда ли, напоминает ситуацию с носителями информации, например, с жесткими дисками. Использованные жесткие диски продают, просто отформатировав их. Или использованные смартфоны просто сбрасывают в заводские настройки. Не так ли?

Шпионы Эрика Справедливого скупали такие пергаменты на рынке пачками, а затем с помощью нехитрых химических реактивов и небольшой магии восстанавливали все что удавалось с них восстановить и получали массу интереснейшей информации. Еще проще это получалось делать с бумажными архивами. Таким образом, разведка Эрика получала более половины всей необходимой информации.

Читателю. Кто-то из вас, несомненно, скажет, мол, фи, копаться в мусоре. Некрасиво. Да. Некрасиво, но эффективно! И это важно! Потому важно использовать правильное уничтожение мусора.

В королевстве Эрика Справедливого был принят другой порядок уничтожения. Особо важные документы, а бумажные – все измельчались на специальных машинах, изобретенных гномами. После них все листы превращались в маленькие квадратики 3х3 мм, а потом бумажные квадратики в запечатанных бумажных же мешках отвозились на бумажные фабрики, где под наблюдением королевских гвардейцев опускались в специальные чаны для изготовления бумаги, а пергаментные остатки – на фабрики, где изготавливались изделия из прессованной кожи. Таким образом, казна получала еще и прибыль от уничтожения мусора.

Читателю. Вам это ничего не напоминает? Пора бы и вам создать свою политику уничтожения информации. Как на бумажных, так и оптических и тем более магнитных носителях!

Сказки о безопасности: Криптография и образование

После того как в королевстве Эрика Справедливого началось широкое использование гномьей и эльфийской криптографии, король заметил, что лица его министра обороны и министра финансов периодически становятся задумчивыми и даже угрюмыми. Поскольку король был очень умным, он решил с ними побеседовать. Вызвал он их обоих как-то и предложил откровенно побеседовать за бокалом хорошего вина.

– Генерал, что вас беспокоит?

– Ваше величество, мы все чаще и чаще используем гномью и эльфийскую криптографию. А что если когда-то они перестанут быть нашими союзниками? Нужно готовить своих криптографов и криптоаналитиков.

– Вот и я о том же думаю, – сказал министр финансов.

Задумался король. Сказал, что они правы, но как быть? Нужно готовить своих специалистов, но как? Откуда их брать? Готовить в университете? Но для этого нужно вначале подготовить преподавателей. Где и как?

Преподаватели информационной безопасности должны быть безусловно свои. Но проблема в том, что готовить преподавателей нужно долго и тщательно. И путь это не близкий.

Решил король отобрать наиболее подготовленных математиков и сделать из них преподавателей. Школьных преподавателей.

Король был умным и понимал, что просто так нельзя принять студентов ниоткуда и если хочешь получить умных специалистов, то нужно начинать со школы.

Нравится вам или нет, но подготовка хорошего преподавателя (инструктора) – процесс длительный, а хороший преподаватель вообще товар штучный. Мало того, что он должен быть умным и подготовленным, он должен уметь и любить преподавать и передавать свои знания. Увы, это часто не получается даже у самых лучших профессионалов.

Прошли годы. Из умных студентов выросли толковые профессионалы. За каждым из них наблюдала специальная служба короля. И через много лет части из них было предложено перейти во вновь организуемую Академию военной службы и безопасности королевства. А для того чтобы они не беспокоились о материальной стороне, король положил каждому из них для начала оклад не менее чем втрое выше получаемого в настоящее время и потребовал, чтобы не менее 20% своего рабочего времени они уделяли своему профессиональному росту.

Преподаватель должен учить и учиться сам. И только тогда он сможет повториться в учениках.

Вы можете спросить – и что было дальше? А дальше уже в этой Академии стали готовить кадры для союзников. Не забывая, впрочем, о том, что копии ключей шифрования нужно держать у себя, ведь сегодня они союзники. А завтра?

Сказки о безопасности: Обучение королевских пентестеров

Однажды на дороге, ведущей в столицу королевства Эрика Справедливого, двое монахов встретили изможденного больного человека, медленно бредущего по дороге. Он был так слаб, что даже не мог говорить. Монахи взяли его с собой, чтобы вылечить в больнице при монастыре. Лечение больного длилось долго и шло очень тяжело. Прошло немало времени прежде чем он выздоровел. Но все же ему удалось выздороветь. Ничего не рассказывал о себе этот человек.

В один из дней он попросился поговорить с настоятелем монастыря. В разговоре он сообщил, что долгое время был атаманом разбойников, грабил крепости и сейфы богатых купцов, пока однажды не заболел и его не бросили умирать на дороге. Он спросил настоятеля, как же ему жить дальше, так как разбойничать и грабить он уже не хочет, а больше ничего делать не умеет. Как жить дальше?

Задумался настоятель и сказал, что ему нужно немного времени, он должен подумать и посоветоваться со своими друзьями. Настоятель не рассказал о том, что до тех пор, пока не стал монахом, он был инструктором в Академии службы безопасности королевства и связи в ней у него остались, ведь бывших безопасников не бывает.

Запомните, что не бывает бывших сотрудников службы безопасности. Они могут быть в отставке, в запасе, но в случае необходимости сразу же перестают быть бывшими!

Прошло немного времени. Как-то вечером настоятель пригласил к себе на беседу бывшего атамана. Вместе с ними в кабинете находился еще один человек, сидевший в темном углу кабинета и молчавший. Настоятель сказал, что это его друг и он хотел бы выслушать бывшего атамана. Долго длился разговор, пока сидевший в темном углу человек не произнес: «Подходит!».

Настоятель улыбнулся и сказал, что бывшему атаману предлагают возглавить новую кафедру в Академии службы безопасности. Это будет кафедра тестирования взломом. Кафедра пентеста. Атаман согласился. Но потребовал, чтобы и он сам, и преподаватели, и слушатели, и все выпускники кафедры пожизненно находились под строгим наблюдением службы безопасности, чтобы всех их дважды в год проверяли и тестировали маги-психологи, чтобы убедиться, что никто из преподавателей и слушателей не сможет применить свои знания во вред королевству, не перейдет на темную сторону. И пусть это означает некоторое лишение свободы и неудобства, но это лучше, чем своими руками воспитывать новых злоумышленников.

Как ни странно, но в вузах, которые учат будущих специалистов по безопасности, отсутствует психологический отбор кандидатов на обучение. Правильно ли это? Наверное, нет, потому что будущий специалист в области информационной безопасности должен быть кристально чист. Мало того, такие же тесты стоит проходить регулярно не только кандидатам, но и сотрудникам. Кто-то из вас может возразить, мол, это не армия. Может вы и правы, да только нет страшнее ничего, чем вор – сотрудник безопасности или правоохранительных органов.

Вот так и появилась в Академии кафедра пентестинга. А вместе с ней – кафедра маговпсихологов. Но это уже другая сказка.

Сказки о безопасности: Королевские инновации и обучение

В королевстве Жадины I специалисты учились только тому, что им нужно сегодня, в данный момент. Увы, но учились они исключительно «методом тыка». Это приводило к тому, что соответствующие приборы и методики работ осваивались кусками, не полностью. Соответственно, мастера никогда не могли в полной мере использовать те или иные технологии.

Вам это ничего не напоминает? А зря. Как правило, системные администраторы учатся также и только некоторые из них (совсем немногие) читают документацию. Это приводит к непропорциональному расходу как усилий, так и рабочего времени.

В королевстве Эрика Справедливого обратили внимание на то что творится у Жадины I, впрочем, они всегда внимательно смотрели на то, что и как творится у соседей.

И сделали правильный вывод. Покупаете новые технологии (новые средства производства) – будьте добры учиться. Ни одна новая технология не может быть внедрена без проведения соответствующего обучения сотрудников. В результате и брака стало куда как меньше, и деньги, потраченные на обучение, быстро возвращались, ведь чем лучше научены сотрудники, тем меньше брака допускается в работе, да и работа делается быстрее и с лучшим качеством.

А вам так не кажется? Ведь если перед внедрением нового программного продукта ваши сотрудники будут обучаться, то ошибок будет гораздо меньше, а значит продукт будет внедрен с меньшими затратами и усилиями. Не так ли?

Сказки о безопасности: Королевский приют безумных, или пропаганда ИБ для пользователей

В королевстве Эрика Справедливого все чаще и чаще внедрялись технологии и устройства, разрабатываемые в королевстве гномов. С одной стороны, это было очень здорово, а с другой – пользователи не успевали понять, какие отрицательные стороны имеют эти технологии и как следует защищать себя от этих отрицательных сторон.

Вам это не напоминает современный мир с его бесконечным числом гаджетов, Интернетом вещей и т. д. Гаджетов и технологий все больше. Они все разнообразнее, а пользователи, увы, все те же.

Все чаще и чаще в компаниях, внедряющих те или иные технологии гномов, были вынуждены организовывать специальные «Приюты безумных», в которых специально обученные люди, называемые няньками, разъясняли сотрудникам, как правильно работать с теми или иными технологиями, чтобы не нанести вред как компании, так и себе самому.

Все чаще и чаще сотрудникам подразделений информационной безопасности необходимо выполнять просветительскую роль, разъясняя пользователям, как необходимо работать и чего бояться в нашем изменчивом мире.

Увы, но очень скоро выяснилось, что одних нянек в «Приютах безумных» катастрофически мало. Технологии и устройства гномов распространялись все быстрее и быстрее. Люди покупали их все охотнее, но работать с этими устройствами и технологиями совершенно не умели. Тогда король издал указ и в королевстве начали печатать брошюры из серии «Технологии для чайников».

Однако со временем выяснилось, что хотя эти брошюры раздавались практически бесплатно, люди, увы, их не читали, а даже те, кто и читали, чаще всего не понимали прочитанное.

На рынках все чаще можно было увидеть подобные сцены.

– Как можно доверять гномам? – вопрошал Баграм Базарный, широко известный в кругах покупателей мочалы. – Их богопротивные устройства расскажут гномам о вас всё-всё-всё, хотите вы того или нет!

– Пора нам создавать своё! – вопил его сосед по лотку Альбрехт, в жизни ни дерева ни вырастивший, ни печи не сложивший, но гномовские гаджеты пользовавший.

Вам это не напоминает ситуацию с компьютерной литературой из серии «Для чайников», впрочем, как и со статьями на популярных ресурсах для пользователей? Вспомните такой ресурс, как , где одни и те же вопросы повторяются изо дня в день. http://answers.microsoft.com

Король задумался. Технологий все больше и больше, как и гаджетов, а думающих все меньше. Да и няньки в «Приютах» все чаще начинают уставать и становиться все более агрессивными. Все чаще и чаще слышны разговоры о том, что кто-то из них не выдержал и наорал, а то и ударил пользователя.

Как быть? Я не знаю. Не знает и король. А вы знаете?

Сказки о безопасности: Рождение социальной сети, или звездный час для спецслужб

В дальней Галактике в планетной системе у звезды Альфа-8 была обитаема Изумрудная планета. Ее когда-то назвали так ввиду мягкого климата и огромного океана с ярко-изумрудной водой.

На планете давным-давно не было государств и войн, а правил император. Планета жила в основном продажей высокотехнологичного оборудования и программного обеспечения. Поскольку она находилась вдали от известных межзвездных путей, то туристы там появлялись весьма редко. Местное население весьма активно использовало для общения планетарную сеть, однако, как неоднократно замечал в своих докладах императору его начальник контрразведки, было глубоко несчастным. Проводимые периодически социологами из контрразведки опросы показывали, что основной причиной несчастья было отсутствие общения. Попытки развивать сеть увеселительных заведений ни к чему не привели. Население просто отказывалось туда ходить, им вполне хватало виртуальной реальности у себя дома. Вместе с тем на планете падала рождаемость. Надо было что-то делать, а что?

И тут разведке пришла идея. Раз уж люди разучились фактически общаться между собой и ушли в виртуальность, нужно сделать так, чтобы они общались в виртуальности. Пришла идея создания социальной сети.

Вам не кажется, что мы тоже постепенно уходим от реального общения? Особенно в больших городах. А зря не кажется!

Идею создания социальной сети первыми, как ни странно, поддержали студенты и… разведка. Вернее, контрразведка. Ведь в таком случае люди, общаясь с компьютерами, становились гораздо более открытыми, особенно если использовали не реальные имена, а ники. Ну а связать ник с реальным человеком не так уж сложно, если знать где и как ковырять.

Прошло несколько лет. Социальная сеть получила широкое распространение, особенно среди молодых людей. А разведка получила огромное количество материалов, позволяющих составлять психологические портреты. Люди стали активнее общаться.

Вместе с тем при приеме на работу стали активнее использовать составленные на базе сообщений социальной сети психологические портреты. А службы безопасности соответствующих компаний стали отслеживать поведение своих пользователей в сети как на работе, так и вне ее.

Будьте умнее. Постарайтесь оставлять минимум данных о себе и своих близких. Помните, что любая фраза может быть и будет использована против вас.

Сказки о безопасности: Социальная сеть пять лет спустя, или как закрыть ящик Пандоры

После прошло пять лет. Вслед за первой появились и другие соцсети. Но тут оказалось, что не все так просто. создания социальной сети на Изумрудной планете

После доклада начальника контрразведки император понял, что после создания социальных сетей они открыли ящик Пандоры. И собственно неприятности только начинаются. Ведь пользователи социальных сетей не думая размещали о себе материалы, которые при внимательном просмотре можно было отнести к категории «Секретно» и даже «Особой важности. Сжечь по прочтении».

Так военнослужащие зачастую сообщали номера и размещение своих воинских частей, фотографии с военных полигонов, на которых они были изображены на фоне совершенно секретной техники. Не лучше обстояли дела и у инженеров и ученых. Зачастую ума хватало обсуждать достоинства и недостатки тех или иных проектов. Более того, даже сотрудники службы государственной безопасности не отличались наличием ума и внимательности!

В ходе развития социальной сети появились банды, использующие материалы социальных сетей для проведения phishing и даже spear phishing атак. То есть уже не только обычное мошенничество пошло в ход, а даже направленные мошеннические атаки. И джина загнать назад в бутылку не представлялось возможным.

Что делать? Как быть?

Император принял решение обучать пользователей методам информационной безопасности прямо со школьной скамьи. Никто не знал, поможет это или нет, но делать что-то надо было.

Задумайтесь, о чем вы пишете в социальных сетях, какие фото выставляете. Ведь вся эта информация – путь к созданию целевой атаки на вас.

Что делать? Запретить социальные сети совсем? Но ведь во многих случаях это несомненная польза. Как быть?

Ответа на этот вопрос у меня нет. Думаю, что польза социальных сетей несомненна. Но и вред тоже налицо. Потому просто прошу вас думать. Почаще и побольше. Джин выпущен из бутылки и назад его загнать нельзя!

Сказки о безопасности. Пришла беда откуда не ждали

После широкого распространения социальной сети на Изумрудной планете казалось, что хуже уже некуда. Но, увы, оказалось, что есть куда. Люди стали сидеть в социальных сетях из дома и с работы. Менеджерам ИТ-компаний показалось что есть рынок для развития. И появились вездесущие гаджеты. Компьютеры стали миниатюрными, в ход пошли планшеты и смартфоны. Если изначально задумывалось что эти устройства будут предназначаться в первую очередь для телефонных переговоров и игр, то теперь, оценив прелесть добывания данных из социальных сетей, в них были встроены модули определения географических координат. Вначале это преподносилось как удобство. Можно было проложить нужный маршрут, увидеть состояние пробок на дорогах, увидеть где в тот или иной момент времени находится ваш ребенок, ваше транспортное средство.

Удобно, закричали пользователи.

Первыми удобство оценили спецслужбы. Теперь по сигналам устройства можно было четко определить где находится нужный объект. Потом это же взяли на вооружение суды и показания гаджета о географическом положении устройства стали доказательством в суде.

Но на этом история не закончилась. Сведения о местоположении пользователя оказались весьма привлекательной информацией для рекламодателей. Ведь насколько удобно, идешь по улице и заранее знаешь, что вот тут сидят твои друзья, а вот тут магазин, в котором продают то или иное, а недалеко ресторан и т. д. Реклама стала целевой. Понятие личной информации просто стало товаром.

Сегодня мы с вами наблюдаем это все и у нас. Личная информация давно уже покупается и продается. А мы с вами просто стали товаром.

Более того, даже появились биржи, которые торгуют этой информацией и чем дальше, тем становится все сложнее.

Люди постепенно привыкли к тому что они товар. А гаджеты получили огромное распространение. Но вопросы приватности уже были никому не интересны. Люди привыкли.

Разве у нас с вами не так? По-моему, так. А как вы считаете?

Сказки о безопасности. Пришла беда откуда не ждали – 2

Мир Изумрудной планеты стал миром гаджетов. Все уже привыкли к тому что их координаты продаются и покупаются. Но, как оказалось, это далеко не все. Очередной находкой, спонсируемой спецслужбами, стало то, что все сведения об отправляемых сообщениях, почте, сведения о телефонных переговорах стали храниться не только в компаниях, обеспечивающих переговоры, а и в самих гаджетах, а главное в их резервных копиях, откуда добыть эти сведения было довольно легко.

Все то же самое мы наблюдаем и у нас. Сообщения, сведения об отправляемой почте, списки контактов, частота звонков тому или иному абоненту хранятся сегодня в смартфоне и добыть их оттуда не представляет особого труда.

Таким образом, все переговоры пользователей Изумрудной планеты оказались под колпаком спецслужб. Осталась лишь прослушка мобильных телефонов. Но и тут проблема была решена кардинально. Несмотря на то, что алгоритм шифрования был выбран достаточно устойчивым, его реализация позволяла осуществить расшифровку в реальном времени. Для перехвата разговоров применялись фальшивые станции сотовой связи. Проблема перехвата была решена. Прослушка пользователей больше не представляла сложности.

Надеюсь читатели понимают, что подобная схема перехвата сообщений и голосового трафика существует и у нас и успешно решается с помощью приборов DRTBox, применяемых полицией штата Калифорния.

Для добывания доказательств из гаджетов применялось специальное программное обеспечение, которое позволяло добывать соответствующие данные, а для тех гаджетов, которые были закрыты куда лучше, применялась другая схема. Похищались пароли к резервным облачным копиям и данные без ведома пользователей добывались оттуда. Постепенно вся планета стала огромным полицейским государством.

Абсолютно аналогично дела обстоят и у нас. Если добывать данные из iPhone и Windows Phone сегодня сложнее, то в ход идет добывание данных из резервных копий. И это совсем не так сложно, как вы думаете.

Сказки о безопасности. Пришла беда откуда не ждали – 3

Социальные сети широко распространились на Изумрудной планете. Наверное, не стало людей, которые не пользовались ними. Но это привело к тому, что большинство людей не думая выкладывали сведения о себе и своих привычках, фотографии как свои, так и своих вещей и прочие сведения как о себе, так и своих друзьях.

Не стал отличием от всех остальных и маленький принц, сын Императора. Он часто рассказывал где и как отдыхал, рассказывал о своей школе, об одноклассниках.

Ну и одноклассники также не отличались благоразумием. И тоже писали о себе и своих друзьях. В том числе и о принце и его жизни.

И в мир Изумрудной планеты пришел spear-phishing.

Spear – phishing – направленное почтовое мошенничество с единственной целью получить несанкционированный доступ к конфиденциальным данным. В отличие от phishing, представляющего собой мошенничество для более широкой аудитории, spear – phishingпредставляет собой более точечное нападение, использующее доверительные данные о клиенте. Часто использует доверительные отношения и умную тактику, привлекая внимание жертв.

Так как с помощью spear – phishing мошенники вызывают большее доверие жертвы, то подобные атаки гораздо успешнее чем простophishing, но требуют куда большей подготовки со стороны мошенников.

Однажды принц потерял свое кольцо, подарок императора ко дню рождения. Принц был очень огорчен этим и не знал, как сказать об этом отцу. Он рассказал об этом друзьям, а вдруг они видели кольцо и смогут ему помочь.

Но тут нашелся выход. По электронной почте, адрес которой он указал в социальной сети, ему пришло письмо, в котором неизвестный благожелатель сообщил, что нашел его кольцо и готов его вернуть за вознаграждение.

В письме также сообщалось, что принцу вернут его кольцо, если он перечислит 20 000 галактических кредитов на указанный анонимный счет. Как только деньги будут перечислены, принцу придет письмо с указанием где он сможет забрать кольцо. Безусловно, это было мошенничество, но принц был так юн, что не мог поверить, что кто-то захочет его обмануть. Да и деньги у него на карте были.

Он так и сделал, перечислив деньги на соответствующий счет в банке. Правда он не знал, что все операции по его счету отслеживались по указанию императора имперской контрразведкой. Специалисты заинтересовались куда и кому перечислены деньги и на всякий случай заблокировали платеж.

Учтите, уважаемый читатель, что вы не принц и всемогущие спецслужбы не будут вам помогать. Если б такое произошло с вами, то деньги бы ушли, и вы никогда бы их не получили обратно.

В результате была арестована банда вымогателей.

А кольцо спросите вы? А кольцо было найдено в комнате принца во время очередной генеральной уборки. Увы, принц, как и большинство мальчишек, не любил наводить порядок в своей комнате.

С тех пор принц больше не пользовался социальными сетями, а его друзьям категорически было запрещено писать о королевской семье.

Надеюсь вы понимаете, что даже если письмо внушает вам доверие, вовсе не обязательно сразу же выполнять то, о чем вас просят.

Как бороться с направленным мошенничеством?

Стоит отметить, что традиционные средства противодействия атакам часто не останавливают подобные нападения, потому что они очень хорошо настраиваются под конкретного получателя. В результате их очень сложно обнаружить. Даже одна ошибка сотрудника, как правило, будет иметь серьезные последствия для компании.

Чтобы бороться с направленным мошенничеством, ваши сотрудники должны осознавать наличие подобных угроз, поддельных электронных писем в своих почтовых ящиках. Помимо образования вам естественно потребуется технология защиты почты.

Сказки о безопасности. Пришла беда откуда не ждали – 4

Не стоит думать, что все беды в Интернет сосредоточены только вокруг социальных сетей. На Изумрудной планете долго думали, что стоит отказаться от публикации фотографий своих путешествий и тут же наступит благодать и к ним перестанут приходить надоедливые рекламные объявления. Да не тут-то было.

Как заметили исследователи из компании «Emerald planet», все большее распространение в планетной сети стало получать новое вредоносное ПО – рекламные приложения.

Рекламные программы – вид шпионского ПО, размещающего на зараженных компьютерах рекламу в виде всплывающих окон, баннеров и т. д.

Вместе с тем появились новые программы-шпионы, собиравшие информацию об активности пользователей в Интернет – какие сайты посещают, как часто, что ищут. Такие программы не размещали никаких объявлений и по сути никакого вредоносного воздействия не вели, не считая, естественно, шпионажа.

Сегодня такая функция есть практически в любом браузере. Стоит вам посмотреть на сайт, посвященный часам и вот уже практически на каждом сайте вас преследует реклама продажи часов…

Избавиться от баннеров и всплывающих окон удалось достаточно быстро путем разработки соответствующего ПО, но как быть с надоедливой рекламой.

И тогда был изобретен специальный режим браузеров In Private. По окончанию сеанса вытиралась вся история посещений в данном сеансе, не сохранялись пароли и прочее. В результате этого вы не получали надоедливую рекламу. Хотя нет, реклама была, но она стала не столь целевой.

Несомненно, вы тоже используете режим In Private? И удаляете всю историю посещений и куки по окончанию сеанса? Нет? Зайдите в настройки вашего браузера и сделайте это немедленно.

А исследователи из «Emerald planet» были награждены премией Императора Изумрудной планеты и им было суждено еще долго и плодотворно работать на благо Империи!

Сказки о безопасности: Королевское шифрование и импортозамещение

В королевстве Эрика Справедливого при проведении телефонных переговоров широко использовались шифрующие устройства, изобретенные гномами. Все было хорошо. И работали они исправно. Да вот беда. Ключи для шифрования тоже генерировались на устройствах от гномов.

Задумался начальник разведки королевства. Хорошо все это, пока мы дружим с гномами. Да и то, мало ли как точно работают эти устройства?

Обратился он к своим специалистам, мол, проверьте. Ха, проверьте. Легко сказать, да сделать как? Специалистов-то нет! Да и исходные коды гномы не дают! Коды-то попросить можно, может и дадут. Да кто ж разберется?

Нужно бы придумать что-то свое. Да. Нужно. Но кто придумает?

Использовать средства иностранной криптографии можно лишь в том случае, если вы безоговорочно доверяете изготовителю. А вот можете ли вы ему доверять и насколько – решать вам и только вам.

Решил король отобрать самых умных студентов университета и послать их учиться в Академию к гномам. Устроить обмен студентами.

Как решил король, так и сделал. Послал одну группу к гномам, а другую к эльфам, стеганографии учиться.

Прошло пять лет, вернулись студенты. И тогда на основе факультета математики создал король закрытую кафедру «Прикладной криптографии», а студенты, которые поумнее оказались, стали там преподавать. Прошло еще несколько лет, и на кафедре был изобретен свой, новый алгоритм шифрования, да и сделаны аппаратные средства, его реализующие.

Так был изобретен новый алгоритм криптографии, а королевство избавилось от страха.

Задумайтесь. При широком распространении алгоритмов криптографии можете ли вы всегда гарантировать бесперебойную работу ваших устройств? Можете ли вы гарантировать, что в некоторое время «Ч» не перестанут работать ваши устройства? Хорошенько задумайтесь!

Сказки о безопасности: как король пароль угадал

На рассмотрение высшего королевского суда Эрика Справедливого была подана жалоба купца Ярека на гномов, а точнее на гномью конструкцию шифрования. Мол, конкуренты читают его переписку и узнают все его замыслы.

«Уж третий раз пароль меняю, – жаловался купец, а подлые конкуренты все равно все знают. То ли гномы им рассказали, как пароли вскрывать, то ли вообще ненадежно это все.»

Ладно бы купец просто написал в суд, да нет, он стал прилюдно об этом кричать на базаре, понося гномов. В результате в высшем королевском суде были две жалобы – самого купца и посольства гномов «О защите чести и достоинства».

Потому это дело и было вынесено в высший суд.

На суде король спросил, мол, кто устанавливает пароль для шифрования? На что купец, возмутившись, сказал, что это делает он сам.

А на вопрос, а каким же был первый пароль, купец ответил, что он мужик умный, потому пароль был «Людмила121116», так как его дочь Людмила родилась 12 ноября 16 года.

Конец ознакомительного фрагмента.