Глава 1

Банальные сентенции

Сфера кибербезопасности переполнена суждениями, которые, может, и звучат разумно и убедительно, но на практике бесполезны и даже контрпродуктивны. К сожалению, их так часто повторяют, что они обрели статус непреложных истин и искажают многие представления об этой сфере и способах добиться в ней эффективных результатов.

Итак, вот три главных, наиболее вредных киберпредрассудка:

— Это все человеческий фактор!
— Спасайте бриллианты короны!
— Киберугрозы не стоят на месте!

Это все человеческий фактор!

«Проблема не в технологиях, а в людях». Иногда это утверждение звучит иначе: «В сфере кибербезопасности человек — самое слабое звено». Хотя люди время от времени забывают флешки в USB-портах, открывают письма

с вредоносными вложениями и в целом ведут себя беспечно, не стоит сводить все беды к этому. За многие возникающие проблемы ответственны сами специалисты по кибербезопасности: они не способны понять поведение рядового пользователя в цифровом мире, к тому же существующая система поощрения недостаточно мотивирует их на качественную работу.

Для полноты картины сравним, как человеческий фактор влияет на обеспечение безопасности в повседневной жизни и в мире компьютерных сетей. Проверим тезис на прочность.

В офлайне мы давно поняли, что определенным сферам, локациям и ситуациям присущи повышенные риски, которым люди не всегда уделяют должное внимание. Чтобы нивелировать влияние опасных факторов, мы принимаем меры по защите и стремимся минимизировать возможный ущерб: например, устанавливаем отбойники на шоссе и «лежачих полицейских» возле школ. Мы учитываем поведенческие паттерны и не обвиняем людей в том, что они... скажем так, порой безответственны и неосторожны. Мы не ожидаем, что они исправятся только потому, что мы рекомендуем это сделать.

В цифровом мире все с точностью до наоборот: мы редко пытаемся уберечь или подстраховать людей от ошибок и необдуманных действий. Зато беспощадно ругаем их за случившееся, а в качестве решения проблемы предлагаем изучить правила компьютерной безопасности.

Тайна потерянной флешки

В 2007–2008 годах в Гонконге имело место девять случаев непреднамеренной утраты личных и медицинских данных граждан — в общей сложности 16 000 человек. В итоге Больничное управление Гонконга обратилось к нам за помощью. Перед нами стояла задача — разобраться в истинных причинах потери данных, скорректировать политику конфиденциальности и предложить меры по улучшению системы безопасности[1].

В одном случае сотрудница администрации в Больнице принца Уэльского (район Новые Территории) оставила флешку в такси. Сделать вывод, что всему виной отсутствие базовых знаний о кибербезопасности, так же легко, как во время просмотра фильма предположить, что человек с пистолетом, стоящий над трупом, и есть убийца.

Чтобы лучше разобраться в причинах инцидента, мы задали девушке всего два вопроса.

1. ***В чем состоят ваши рабочие обязанности?***

Как оказалось, сотрудница выставляла другим госпиталям счета за проведение клинических исследований в лабораториях больницы.

2. ***Зачем вы копируете информацию на флешку?***

В действиях девушки не было ничего ужасного; они диктовались логикой; многие сотрудники крупных компаний сталкиваются с подобным. На ее компьютере отсутствовала нужная для работы программа Excel. Поэтому она копировала

[1] "Report of the Hospital Authority Taskforce on Patient Data Security and Privacy," http://www.ha.org.hk/haho/ho/hesd/Full_Report.pdf.

на флешку электронные таблицы, полученные от других больниц, а затем переносила на компьютер коллеги, у которого Excel был. При этом она постоянно и безуспешно просила IT-отдел установить Excel на ее компьютер.

Итак, всему виной действительно человеческий фактор, но связанный не с делопроизводителем, а с сотрудниками IT-отдела, не удосужившимися установить коллеге необходимую программу. Когда они это сделали, риск утечки данных из-за потери флешки исчез, поскольку отпала потребность ее использовать.

Пример показывает, что люди стремятся хорошо выполнить свою работу, даже если при этом нарушают требования безопасности. Девушка не осознавала, что ставит под угрозу данные пациентов. Она просто не нашла другого решения проблемы.

Фишинг, бессмысленный и беспощадный

Люди часто открывают вложения в электронных письмах и кликают по ссылкам, что приводит к установке шпионских программ. Хакеры стали куда умнее: они нередко используют в рассылках информацию, почерпнутую из социальных и профессиональных сетей, а потому отличить фишинговые письма от обычных все труднее. Хотя несколько нигерийских принцев все еще жаждут вручить вам миллионы долларов, их сообщения постепенно вытесняются другими, гораздо более убедительными.

Калифорнийский университет в Беркли собирает базу данных о фишинговых атаках и пополняет ее образцами таких посланий. Нашлось даже поддельное письмо от HR-отдела самого университета (рисунок 1)[2].

Рисунок 1. Пример фишинговой атаки

От: <HR@berkeley.edu> <HR@berkeley.edu>

Subject: Message from human resources

Дата: 13 апреля 2017 Время: 21:29:54

Кому: XXXXX@berkeley.edu

Уважаемый XXXXX@berkeley.edu

Информационное письмо направлено HR-отделом.

Пройдите по этой ссылке, чтобы авторизоваться и просмотреть документ. Спасибо!

Калифорнийский университет в Беркли, HR-отдел.

[2] Berkeley Information Security Office, "Phishing Example: Message from Human Resources," https://security.berkeley.edu/news/phishing-example-message-human-resources.

Письмо кажется настоящим. Просьба авторизоваться для просмотра документа не вызывает подозрений: это стандартная практика для многих организаций, особенно при работе с конфиденциальной информацией. Отдел IT-безопасности университета Беркли в данном случае порекомендовал проверять достоверность ссылки, прежде чем переходить по ней. Наведите на нее курсор, и внизу экрана появится адрес веб-сайта. Затем нужно убедиться, что ссылка действительно ведет на страницу HR-отдела, а не на ресурс мошенников.

Такой совет одобрило бы большинство экспертов по кибербезопасности, но есть два нюанса. Во-первых, просмотр рабочих писем — рутина, с которой часто хочется покончить побыстрее. Многие решат, что наведение курсора на ссылку, изучение и проверка веб-адреса займут слишком много времени. Во-вторых, далеко не каждый рядовой пользователь сумеет проверить достоверность веб-адреса. Компания не может вменять это сотрудникам в обязанность.

Обучение основам безопасности

Это распространенный способ снизить риски фишинговых атак и внедрения вредоносного ПО в корпоративные компьютерные сети. Однако даже сотрудники компаний, специализирующихся на кибербезопасности, не могут похвастаться блестящими результатами подобных тренингов. Компания Intel Security (в прошлом McAfee)

протестировала 19 000 человек в 140 странах, и только 3% из них выявили все фишинговые имейлы в выборке из десяти сообщений, а 80% не нашли ни одного[3]. Никакое обучение основам безопасности не решит эту проблему: достаточно одному сотруднику кликнуть на вредоносную ссылку или зараженное вложение, чтобы фишинговая атака достигла своей цели.

Отстрел на подлете

Еще один инструмент борьбы с фишингом — современные технологии, предназначенные для выявления вредоносного ПО заранее, на этапе установки. Но как гарантированно поймать всех воров и шпионов? Первоначально здесь помогало составление списка сигнатур, то есть своего рода отпечатков пальцев известных образцов вредоносных программ, и их сравнение. Новая программа не прошла проверку на «отпечатки пальцев»? Система безопасности блокирует запуск. Продвинутые антивирусы принимают во внимание также дополнительные характеристики, в том числе поведение потенциально вредоносного ПО. Однако проблема остается, и разработчики антивирусов пытаются своевременно обновлять свои продукты, не отставая от ухищрений хакеров.

---

[3] Tom Reeve, “Even Security Experts Fail to Spot Phishing Emails, Finds Report,” SC Media, May 19, 2015, https://www.scmagazineuk.com/even-securityexperts-fail-to-spot-phishing-emails-finds-report/article/537183/.