ЭФФЕКТИВНЫЕ МЕТОДЫ БОРЬБЫ С ФИШИНГОВЫМИ АТАКАМИ. ЧАСТЬ II.

ПРОДОЛЖЕНИЕ. НАЧАЛО В INFORMATION SECURITY, №1 , ФЕВРАЛЬ-МАРТ, 2009

НОВЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Описанные выше методы противодействия фишинговым атакам, особенно применяемые совместно, позволяют повысить безопасность, однако в любом случае остаются подверженными тем или иным видам атак и при известной настойчивости злоумышленника не смогут защитить деньги и данные пользователя.

Уже рассмотренные способы обладают одним общим недостатком – применяемые меры легко сводятся на нет небрежностью или не внимательностью пользователя. Согласие принять сертификат, подписанный недоверенным УЦ или переход по ссылке из спамового письма на поддельный сайт вообще без установления защищённого SSL-соединения, несвоевременно обновлённые базы персонального антивируса, неправильно настроенный локальный файрвол, введённые три подряд идущие одноразовые пароли на фишерском сайте, то же согласие выбрать новую картинку для сайта или игнорирование сообщение о невозможности загрузить её – всё это и многое другое в конечном итоге может привести и, к сожалению, приводит к потере денег.

Как правило, в договорах, заключаемых с пользователями платёжных систем или клиентами банков, вся ответственность за халатность в действиях возлагается на самих пользователей. Попытка таким образом обезопасить себя юридически уже приводит к ответным действиям клиентов. Не редкостью становятся судебные процессы, в которых адвокаты доказывают, что при имеющейся системе аутентификации обеспечить сохранность данных клиент был не в состоянии, о чём в момент заключения договора сотрудники банка не могли не знать, а значит, и возложение ответственности было не правомочным. С другой стороны, потеря денег пользователями, пусть даже по своей вине в любом случае негативно сказывается на репутации банка в их глазах, а при массовых потерях – так же и в глазах ещё не пострадавших клиентов.

Рассмотри методы борьбы с фишинговыми атаками, представляющиеся наиболее эффективными на сегодняшний день и лишенные описанных выше недостатков.

ПРОПАГАНДА КУЛЬТУРЫ ПОВЕДЕНИЯ

Как мы уже выяснили, самое слабое звено в современных системах защиты вообще и от фишинговых атак в частности это человек. Именно поэтому, важнейшее внимание компании, обеспокоенной потенциальными потерями денег, стоит обратить на пропаганду основ информационной безопасности среди своих сотрудников и клиентов.

Приведём некоторые из правил, рассказам о которых стоит уделить чуть больше внимания, чем простое упоминание на предпоследней странице многостраничного договора на обслуживания.

- Не доверяйте ссылкам в электронных письмах;
- Не отправляйте личную информацию в ответ на просьбу по электронной почте;
- Проверяйте правильность URL-адреса;
- Вводите адрес в строку браузера самостоятельно;
- Используйте только телефонные номера, указанные на кредитной карте или в договоре;
- Не открывайте неизвестных вложений в письмах.

Возможно, кому-то этот список покажется элементарным, но если говорить о пользователях в целом, то общепринятое выполнение даже таких простых правил способно существенно уменьшить доходы фишеров, потенциально сделав данный бизнес менее рентабельным, а значит, менее привлекательным. Правила дорожного движения, особенно для пешеходов, тоже нельзя назвать сверхсложными, но всеобщее их знание и более-менее выполнение ежегодно спасает немало жизней.

Понятно, что в масштабах государства пропаганда правил компьютерной безопасности не является столь высокоприоритетной задачей, и именно поэтому основная надежда здесь на руководителей организацией. Ведь именно их бизнесу и их деньгам напрямую через сотрудников или опосредованно через клиентов угрожают фишеры.

ПРОТИВОДЕЙСТВИЕ ФИШИНГУ В КОРПОРАТИВНОЙ СРЕДЕ

Основным приоритетом при построении защиты от фишинга в рамках компании стоит сделать максимальный уход от человеческого фактора. Именно поэтому наиболее перспективными представляются шлюзовые решения, которые в отличие от персональных продуктов не только снижают нагрузку на рабочие станции и упрощают администрирование, но и позволяют закрыть всю компьютерную сеть организации единым надёжным «зонтиком».

Современные эффективные шлюзовые решения борются с фишерскими атаками на четырёх уровнях:

- **Уровень доступа**. Основа антифишинговой безопасности – это уже рассмотренная URL-фильтрация (запрет доступа к сайтам из категории фишинговых), которая, несмотря на свою низкую эффективность «в бою один на один», дополненная рядом технологий, позволяющих отличить ссылку на фишерский сайт от легитимной, способна оказать сопротивление фишерам.
- **Уровень активного контента**. Лучшие в этом классе решения реализуют фильтрацию 100% HTML-кода и внедренных объектов на наличие вредоносного кода, в том числе скрытых каскадных переадресаций, когда тело трояна собирается из небольших безвредных по отдельности фрагментов и потому трудно детектируемых частей на нескольких сайтах, по которым пользователя прозрачно для него «пробрасывают». Благодаря эффективной очистке трафика реализуется защита пользователя от потенциальных нежелательных последствий в случае состоявшегося всё же перехода на фишерский сайт.
- **Уровень коммуникаций**. В том случае, когда целью привлечения пользователя на поддельный сайт является заражение его компьютера каким-либо вредоносным кодом, ещё одним уровнем блокировки защиты быть предотвращение передачи приватных данных, собранных ботами. Несмотря на большое количество и огромное разнообразие видов самих троянов и ботов, существует всего лишь несколько десятков коммуникационных протоколов, по которым они взаимодействуют со своим управляющим центром. Таким образом, блокировка таких коммуникаций наиболее эффективно осуществляется по сигнатурам протоколов, а не самого вредоносного кода.
- **Уровень передачи данных**. Получившие широкое распространение в последние годы DLP-решения (Data Leak Prevention) позволяют в рамках компании построить ещё один рубеж обороны в виде контроля потенциальных каналов утечки данных. Такие решения могут помочь в выявлении и предотвращении отправки вредоносным кодом, например, номера кредитных карт или другую конфиденциальную информацию.

Пожалуй, единственным слабым местом таких систем может оказаться невозможность защиты мобильных сотрудников, работающих удаленно по открытым каналам связи. Для решения данной проблемы в качестве одного из вариантов можно предложить проксирование, т.е. выход в интернет с ноутбуков компании только через головной офис. Такое же решение для упрощения администрирования и снижения финансовых затрат можно предложить и для филиалов. Стоит отметить, что ведущие игроки этого сегмента рынка готовы предложить своим клиентам самим почувствовать себя в роли таких филиалов, предлагая не приобретать и

сопровождать их продукты, а арендовать для фильтрации почтового и веб-трафика вычислительные мощности самого производителя.

ПРОТИВОДЕЙСТВИЕ ФИШИНГУ КАК КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО

Помимо заботы о собственной конфиденциальной информации и защите сотрудников в филиалах и офисах многие компании заботятся и о своих клиентах. Деловая репутация порой стоит дороже, чем затраты на построение действительно безопасной системы по аутентификации пользователей.

Уже рассмотренный ранее протокол SSL имеет возможность проводить двустороннюю аутентификацию, когда проверяется валидность не только сервера, но и самого пользователя. Для этого клиентам, например, банка необходимо получить цифровой сертификат. Сделать это можно, как правило, при заключении договора на обслуживание или позже в любое время.

Отказ от паролей при доступе пользователей к счетам серьёзно осложняет жизнь фишерам. Использование цифровых сертификатов на стороне сервера и клиента снимает проблему атаки «человек посередине» и делает прослушивание и перехват трафика бесполезными.

Основой безопасности при использовании цифровых сертификатов является сохранность закрытого ключа. Организация имеет гораздо больше, чем рядовой пользователь, финансовых и технических возможностей по надежной защите закрытого ключа, используемого для аутентификации её веб-сайта. Хранение клиентом своего закрытого ключа в реестре операционной системе или на жёстком диске не является безопасным. В случае заражения компьютера пользователя эти данные легко могут быть похищены вредоносным программным обеспечением, и защита закрытого ключа паролем не будет являться надёжной гарантией сохранности денег пользователя. Применяемые на практике пароли редко превышают 8 символов и зачастую если и не являются осмысленным словом, то состоят только из прописных букв латинского алфавита.

Самым надёжным способом хранения закрытых ключей пользователя на сегодняшний день является использование криптографических токенов. В отличие от других внешних носителей (например, тех же USB-флэш) при использовании токенов нет необходимости в копировании секретной информации в оперативную память компьютера при проведении операции аутентификации, так как подобные устройств не только надежно хранят закрытые ключи, но и аппаратно выполняют необходимые криптографические вычисления. При этом важно, что воспользоваться токеном может только его владелец, знающий пароль от него (пин-код).

Многие банки уже сегодня предлагают своим клиентам возможность аутентификации не только по одноразовым паролям, но и с использованием цифровых сертификатов. Однако пока не так широко распространено использование аппаратных криптографических токенов для повышения безопасности хранения закрытых ключей, тем не менее и таких банков становится с каждым годом всё больше, ведь данный механизм на сегодня является без сомнения одним из самых надёжных для аутентификации при осуществлении он-лайн транзакций.

ЗАКЛЮЧЕНИЕ

Имеющиеся сегодня как хорошо и давно известные, так и появившиеся в последние годы новые эффективные средства борьбы с фишинговыми атаками, способны свести риски потери конфиденциальной информации пользователей к минимальным значениям. В силу особенности реализации он-лайн сервисов основная работа по обеспечению безопасности данных пользователей ложится на владельцев веб-сайтов. Применяемые ими решения с каждым годом становятся все более надежными, особенно в сфере телебанкига. Однако, до внедрения той же аппаратной аутентификации пользователей в таких сервисах как интернет-аукционы, веб-почта или социальные сети пока ещё далеко, а значит, вполне вероятным представляется всё большая концентрация фишеров именно на них. Говорят, что надёжный замок остановит злоумышленника не столько сложностью его взлома, сколько возможностью выбора вором соседней двери с более простым механизмом закрытия. Именно поэтому для банков, заботящихся о своих клиентах, очевидным является необходимость применения именно надёжных и эффективных методов борьбы с фишерами.