Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Проблема
- Решение
- Примеры

Двухфакторная Аутентификация

ОБ АВТОРЕ

Фред Кирби - гость этого номера. Фред является старшим преподавателем Института SANS, читает курсы «Введение в информационную безопасность (SEC301)», «Управление информационной безопасностью (MGT512)» и «Основы безопасности (SEC401)». Ранее Фред работал менеджером информационного департамента ВМФ США Naval Surface Warfare Center Dahlgren Division.

ПРОБЛЕМА

Чтобы воспользоваться различными услугами в Интернет, например, электронной почтой, онлайн банкингом или совершить покупки, мы, прежде всего, должны доказать, что мы тот человек, за которого себя выдаем. Данный процесс удостоверения личности называется аутентификацией. Аутентификация может осуществляться с помощью того, что вы знаете (например, пароль); того, что у вас есть (например, смартфон) или одной из ваших уникальных биологических особенностей (например, сканирование сетчатки глаза или отпечатка пальцев). Традиционно используется самый распространённый способ аутентификации с помощью имени пользователя и пароля. Этот способ аутентификации имеет один существенный недостаток: злоумышленнику достаточно подобрать или узнать ваш пароль и он получит доступ к онлайн-счету и конфиденциальной информации. Если вы используете одинаковый пароль и логин для нескольких учётных записей, то ущерб будет существенно больше. Для улучшения защиты учётных записей, интернет сервисы начинают использовать более надёжные методы аутентификации, включающие в себя использование более чем одного фактора аутентификации. Сегодня мы расскажем о том, как это работает и о преимуществах данного метода.

РЕШЕНИЕ

При методе усиленной аутентификации используется более чем один фактор: вы должны не только знать что-то, например, пароль, но и иметь что-то, например, смартфон, или предоставить уникальную информацию о себе, например, отпечатки пальцев. В названии

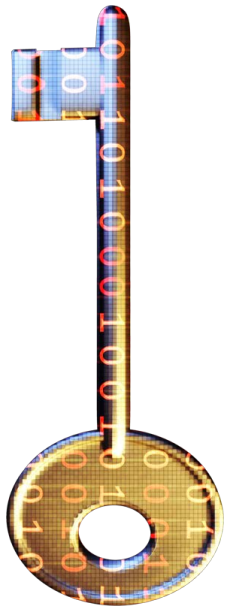
Двухфакторная Аутентификация

термина заключена суть: используется два фактора для аутентификации личности, а не один. Типичным примером двухфакторной аутентификации является работа банкомата. Чтобы получить доступ к услугам банкомата нужно иметь что-то (банковскую карту) и знать что-то (ПИН-код). Если злоумышленники украдут карту, они не смогут ей воспользоваться без ПИН кода (вот почему не стоит писать ПИН код на карте). Использование двух факторов для аутентификации является более надежной защитой.

Метод двухфакторной защиты работает в Интернет аналогично работе банкомата с картой и ПИН кодом. Вы можете использовать логин и пароль для доступа к онлайн аккаунтам. Однако, после успешного ввода пароля, сайт не предоставляет доступ к вашей учётной записи, а запрашивает второй фактор аутентификации, например, проверочный код или отпечатки пальцев. Если у вас нет второго фактора, вы не получите доступ к учётной записи. Это второй уровень вашей защиты. Даже если злоумышленники подберут пароль, то вы и ваша учётная запись по-прежнему в безопасности, так как преступники не смогут совершить второй шаг для получения доступа к информации.

ПРИМЕРЫ

Давайте рассмотрим примеры работы двухфакторной аутентификации. Одним из самых популярных сервисов является Gmail. Многие люди используют логин и пароль для доступа к почте Gmail или других сервисов Google. Теперь Google предлагает возможность дополнительной защиты с помощью двухфакторной аутентификации или, по



Используйте двухфакторную аутентификацию всякий раз, когда это возможно. Это один из самых надёжных способов защиты ваших учётных записей и информации.

версии Google, двухступенчатой проверки. Двухступенчатая проверка Google требует две вещи для аутентификации: пароль (то, что вы знаете) и смартфон (то, что у вас есть). В качестве подтверждения Google каждый раз будет отправлять вам смс с уникальным одноразовым паролем (в некоторых случаях за смс-сообщения может взиматься плата; уточните ваш тарифный план). Именно этот пароль вам и нужно будет вводить. Или вы можете установить приложение, которое будет генерировать такие пароли, вместо смс-сообщений. В этом случае не нужно пользоваться услугами

Двухфакторная Аутентификация

провайдеров связи. Ценность подобного способа усиленной аутентификации состоит в том, что даже в случае если злоумышленники взломают ваш пароль, они не смогут получить доступ к вашим учётным записям Google без физического доступа к смартфону. Таким образом, вы и ваша информация защищены.

Помните, что коды подтверждения, которые вы будете получать в виде смс-сообщений, уникальны и при каждой аутентификации отличаются. Так что вам придется проходить двухступенчатую проверку при каждом входе в сервис. Эта услуга не включена по умолчанию. Чтобы её подключить, нужно войти в вашу учётную запись Google и в настройках безопасности выбрать опцию двухступенчатой проверки.

Другие интернет-сайты тоже предлагают опцию двухфакторной аутентификации, например, Dropbox, Paypal или, возможно, сайт вашего банка. Некоторыми услугами вы можете пользоваться с помощью смартфона, для других необходимо специальное приложение, которое будет генерировать уникальные коды. Также, сайты могут потребовать специальное устройство, которое подключается через USB порт к компьютеру, например, Yubikey. Если онлайн сервисы, которыми вы пользуетесь, предоставляют услугу двухфакторной аутентификации, настоятельно рекомендуем её использовать.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

Двухступенчатая верификация Google:
http://preview.tinyurl.com/cncte9n

PayPal (and EBay) Security Key:
http://preview.tinyurl.com/838dpds

Термины по Информационной безопасности:
http://preview.tinyurl.com/6wkpae5

Ежедневные советы Института SANS по безопасности:
http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков