OUCH! Январь 2023

SANS SECURITY AWARENESS

Ежемесячный информационный бюллетень по безопасности

Биометрия – как сделать безопасность проще

Обзор

Вам не нравятся пароли? Вы устали от постоянного входа на новые веб-сайты или не можете вспомнить все свои сложные пароли? Разочарованы необходимостью генерировать новые пароли для новых учетных записей или изменять старые пароли для существующих учетных записей? У нас есть хорошие новости для вас. Существует решение под названием биометрия, которое помогает вам упростить кибербезопасность. Ниже мы объясним, что такое биометрические данные, как они упрощают вашу жизнь и почему вы станете чаще их видеть.

Во-первых, почему пароли?

Пароли являются частью так называемой аутентификации, процесса подтверждения того, кто вы есть. Как правило, вы можете предоставить две вещи, подтверждающие вашу личность: что-то, что вы знаете (например, ваши пароли) и что-то, что у вас есть (например, карта банкомата или ваше мобильное устройство). Традиционно аутентификация выполнялась с помощью паролей. Сначала были приняты пароли, поскольку это было одно из самых простых решений для аутентификации. Однако с годами наша жизнь стала намного сложнее, и учетных записей стало гораздо больше, чем кто-либо мог ожидать. Довольно часто у человека бывает более 100 паролей на работе и в личной жизни.

Кроме того, кибер-злоумышленники научились угадывать, красть или взламывать пароли. Вот почему вы видите так много правил о паролях, таких как их длина (чтобы их было трудно угадать) и использование уникального пароля для каждой учетной записи (чтобы, если одна из ваших учетных записей была взломана, другие ваши учетные записи все еще были в безопасности). Проблема со всеми требованиями к паролям заключается в том, что они усложняют кибербезопасность. Менеджеры паролей очень помогают, поскольку они надежно запоминают все ваши пароли и регистрируют на веб-сайтах для вас, но есть ли лучший способ? Именно здесь биометрия может помочь, предоставляя третью опцию для подтверждения вашей личности — то, кем вы являетесь.

Биометрия

Как и пароли, биометрия — еще один способ доказать, кто вы есть. Разница в том, что вместо того, чтобы помнить что-то (например, пароли), вы используете элемент того, кто вы есть, чтобы подтвердить свою личность, например, используя отпечаток пальца, чтобы получить доступ к вашему телефону.

Биометрия намного проще, так как вам не нужно ничего запоминать или вводить, вы просто аутентифицируетесь, используя то, кто вы есть. Существует множество различных типов биометрических данных, таких как ваш голос, походка или отпечатки радужной оболочки глаза. Тем не менее, отпечатки пальцев и распознавание лиц являются двумя наиболее распространенными, особенно для мобильных устройств. Хотя у биометрии есть огромное количество преимуществ, у нее также есть некоторые недостатки, один из самых больших заключается в том, что если ваш отпечаток пальца или лицо скопировано кибер-злоумышленниками, вы не сможете их изменить.

Ключи доступа

В ближайшие месяцы и годы вы должны увидеть, как биометрические данные заменяют пароли новой технологией под названием Passkeys. Эта технология используется Microsoft, Apple и Google, и вскоре вы увидите, что она будет применяться на все большем количестве веб-сайтов. Ключи доступа заменяют пароли, позволяя вам подтвердить, кто вы, просто используя биометрические данные в сочетании с вашим мобильным устройством. Когда вы создаете учетную запись на веб-сайте (например, Google или Apple), вместо создания пароля вы регистрируете свое мобильное устройство. Двигаясь вперед, вы входите на этот веб-сайт, аутентифицируясь на своем мобильном устройстве с помощью биометрических данных, таких как отпечаток пальца или распознавание лица. Веб-сайт доверяет вашему мобильному устройству, и ваше мобильное устройство подтверждает, что это вы, используя биометрию. Кроме того, ваши биометрические данные (отпечаток пальца или лицо) не отправляются ни на один веб-сайт. Вместо этого ваши биометрические данные надежно хранятся локально на вашем устройстве. Он просто используется для разблокировки «Ключа доступа», уникального ключа, созданного для каждого сайта, который ваше устройство отправляет на сайт, защищая ваши биометрические данные. Хотя идеального решения не существует, биометрические данные и такие решения, как коды доступа, могут помочь обеспечить вашу безопасность и упростить безопасность.

Приглашенный редактор

Доктор Йоханнес Ульрих является деканом по исследованиям в колледже Технологического института SANS. Обладая более чем 20-летним опытом работы в отрасли, в настоящее время он отслеживает текущие угрозы с помощью SANS Internet Storm Center. Он преподает SEC522 (безопасность веб-приложений) и SEC503 (обнаружение вторжений).
Твиттер: @johullrich & LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Ресурсы

Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/
Подробнее о ключах доступа: https://www.sans.org/blog/what-is-phishing-resistant-mfa/

Роман Полаков