БЕЗПЕКА ДАНИХ КОРИСТУВАЧІВ ПРИ ВИКОРИСТАННІ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

Богуцький Д. Б., ст. (гр. КП-81мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Питання безпеки даних користувачів є дуже важливим при використанні двофакторної аутентифікації при реєстрації або авторизації в сучасних веб-застосунках. Тези описують проблеми та ризики використання технології багатофакторної аутентифікації на прикладі двофакторної, адже безпека даних користувачів в мережі Інтернет є найголовнішим завданням, над яким працюють найкращі програмісти світу.

Ключові слова: токен, інтерфейс, аутентифікація, фішинг, кібер-шахраї, акаунт, шифрування.

Abstract: The issue of user data security is very important when using two-factor authentication when registering or authorizing in modern web applications. The thesis describes the problems and risks of using multi-factor authentication technology as an example of two-factor, since the safety of users' data on the Internet is the most important task that the best programmers in the world are working on.

Keywords: token, interface, authentication, phishing, cyber-crooks, account, encryption.

Двофакторна аутентифікація (2FA) – це спосіб ідентифікації користувачів у будь-якому веб-сервісі або веб-застосунку, котрий використовує два різних типи аутентифікаційних даних.

Після ситуації, коли зловмисники викрали доступ до поштових скриньок відомих політиків та акаунтів світових зірок кінематографу, люди стали уважніше дбати про власну безпеку в Інтернеті. Двофакторна аутентифікація стала великим досягненням у сфері безпеки і тепер нею користуються мільйони людей у всьому світі.Всі сучасні компанії почали використовувати цю технологію авторизації в своїх веб-застосунках.

Проте інколи зловмисники полюють не тільки на ваш логін і пароль, але й на код підтвердження, необхідний для входу в акаунт. На сьогодні персональна профіль користувача не може вважатися захищеним без двофакторної аутентифікації. Цю функцію потрібно вмикати всюди, адже вона зменшує ризик взлому вашого акаунту та збільшує безпеку облікового запису.

Взагалі, що значать так звані «два фактори»? «Першим фактором» є логін та пароль, а «другим фактором» може бути як код підтвердження, який генерується в спеціальному додатку у смартфоні користувача, так і просте SMS-повідомлення, що генерує простий код пароль.

Слід відокремити основні переваги використання двофакторної аутентифікації:

– захист одноразовим ключем за допомогою підтвердження через смартфоні;

– не потрібні додаткові токени, адже зараз смартфон у всіх під рукою;

Також є і недоліки використання двофакторної аутентифікації:

– потрібно щоб мобільний телефон користувача мав доступ до мережі Інтернет, коли відбувається авторизація, тому що повідомлення з паролем просто не дійде до смартфоні;

– можливість перехвату повідомлення з кодом підтвердження;

– деякі повідомлення надходять з затримкою, за цей час сервер перевіряє унікальність;

– при афішування свого особистого номеру телефона є ймовірність отримання спаму в майбутньому.

Обхід захисту двофакторної аутентифікації дуже складний процес. Якщо намагатися перехватити текстове повідомлення з додатка користувача, можна змарнувати багато часу. Але це можливо.

Отже, щоб отримати доступ до акаунту «жертви», треба знати її логін, пароль, та унікальний код-пароль, що генерується кожні 10 секунд у мобільному телефоні користувача. Це вже складніше, чи не так? Але все одно, кожен день зловмисники створюють нові, більш хитрі способи обходу двофакторної аутентифікації. Основним ризиком тут є так званий фішинг.

Фішинг являє собою викрадення персональних даних користувачів таким чином, що вони самі розкривають свої дані, навіть не підозрюючи про це.

Шахраї використовують різні виверти, які в більшості випадків змушують користувачів розкривати свої дані самостійно. Наприклад це може бути звичайний електронний лист з проханням підтвердити реєстрацію свого облікового запису. Але в це посилання вшите інше посилання, що веде користувача на відомий йому ресурс, де він вводить свої дані, навіть не підозрюючи про те, що ця сторінка є несправжньою.

Якщо користувач не буде достатньо пильним і введе всі свої данні на фішинговій сторінці, то він дасть змогу шахраям ввійти до його акаунту, а це значить, що вони отримають повний доступ до всієїінформації в обліковому записі.

Існує і такий вид фішингу, котрий може дізнатися у користувача і пароль, і код підтвердження з додатку. Але такі види фішингу є доволі рідким явищем, частіше за все їх роблять спеціально для взломувпливових керівників різних компаній, щоб вилучити з їх акаунтів конфіденційну інформацію або компромат на їх компанію.

Дані користувачів можуть опинитися в зоні ризику, якщо вони:

– використовують єдиний пароль на різних сайтах;

– завантажують програми та файли з непровірених ресурсів;

– переходять по посиланням в електронних листах.

Викрадення пароля може створити багато загроз не тільки користувачу, а і всім, з ким він контактує в Інтернеті. Якщо зловмисник отримає ваш пароль, він зможе завдати немалої шкоди:

– прочитати ваші повідомлення, подивитися особисті фотографії, або навіть видалити їх;

– розіслати от вашого імені образливі повідомлення, спам або віруси;

– змінити паролі до інших акаунтів, якими ви користуєтесь (наприклад, в інтернет-магазинах або онлайн-банках);

– вимагати грошей у ваших знайомих від вашого імені.

Налаштування безпеки не займе багато часу, але ви будете вдячні, якщо ці дії не дозволять зловмиснику отримати доступ до ваших персональних даних.

Щоб не стати жертвою кібер-шахраїв, треба насамперед бути уважним при введені своїх даних на сторінках в Інтернеті. Щоразу треба перевіряти адресу веб-сторінки. Наприклад найпоширеніша фішингова сторінка в Інтернеті має зайві або подвійні літери в своїй адресі. Також компанія Google створила застосунок для захисту персональних даних на фішингових сторінках під назвою «Захисник пароля Google».

Цей застосунок не дає змогу користувачу перейти на сайт при натисканні на фішингове посилання. Застосунок одразу виведе на екран повідомлення, яке попередить про те, що форма введення логіну та паролю на цій сторінці є несправжньою.

Також не ввімкнене шифрування HTTPS повинно відштовхнути користувача від введення своїх персональних даних на цьому ресурсі. Але все одно немає залізної гарантії, що цей або інший застосунок захистить користувача від різних видів шахрайства. Взагалі є і різні платні засоби захисту від фішингу, але вони не такі популярні, як «Google authenticator» або «Google passwordalert».

Отже, для ефективного захисту своїх персональних даних від фішингу користувачу слід налаштувати двофакторну аутентифікацію та самостійно розпізнавати фішингові сторінки, електронні листи та повідомлення. Цього буде досить для базової безпеки та захисту від фішингу.

Як бачите, в користуванні двофакторної аутентифікацією є деякі нюанси, але складними вони здаються тільки на перший погляд. Все одно кожен вирішує для себе сам, яким повинно бути ідеальне відношення безпеки і зручності. Але в будь-якому випадку всі дії виправдовуються в повній мірі, коли справа заходить про безпеку платіжних даних або особистої інформації, не призначеної для чужих очей.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. BrentWilliams. «Identity Lifecycle».
2. Eric Grosse, MayankUpadhyay, Authentication at Scale. IEEE Security and Privacy, January/February 2013.
3. Maria Korolov. 93% of phishing emails are now ransomware. CSO. 2016
4. John Biggs. How to buypass 2FA.