потрібно провести взаємоузгоджене об'єднання і зберігання об'єктів обліку, банків даних, що знаходяться в різних інформаційних системах, створити загальну систему нормативно-довідкової інформації, класифікації та кодування, організувати взаємозв'язок інформаційних систем.

Тут досить зримо проявляється перевага хмарних технологій зберігання даних, що дозволяють здійснювати доступ до віддалених баз даних і використовувати інформаційну потужність хмарних серверів з мобільних пристроїв будь-якого типу.

Мирошниченко В.О.
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ,
к.т.н., доцент

ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КЛІЄНТІВ У ФІНАНСОВІЙ СФЕРІ

У міру того як світ стає все більш цифровим, кількість паролів, які люди повинні пам'ятати, стає серйозною проблемою. Фінансові установи поступово змушені вивчати прийнятні альтернативи біометричної аутентифікації користувачів і врівноважувати обидві важливі змінні: простоту і безпеку.

Суть проблеми полягає в тому, що чим більше сервісів ми використовуємо, тим більше паролів ми змушені запам'ятовувати. Фактично, за оцінками дослідників, протягом наступних п'яти років у кожної людини буде в середньому понад 200 облікових записів, які потребують паролів. Управління зростаючою кількістю паролів стає проблемою майже для всіх користувачів. У відповідь ми можемо спостерігати кілька різних підходів до цього:

• Використання однакових паролів для всіх облікових записів. Очевидно, це найгірше через «ефекту доміно», яке призводить до злому одного аккаунта при атаці.

• Використання різних варіантів паролів. Це поєднання більш високого рівня безпеки з відносною простотою.

• Використання технологій, які генерують надійні паролі. Це найбезпечніший варіант, але і самий громіздкий у використанні.

Згідно з дослідженням, проведеним компанією TeleSign [1], яка забезпечує захист найбільших онлайн-майданчиків, мобільних додатків і хмарних систем, встановлюючи і перевіряючи мобільну ідентифікацію, 73% дорослого населення США і Великобританії використовують один і той же пароль для всього. Крім того, більше половини користувачів (54%) використовують п'ять або менше паролів, а

22% використовують тільки три або менше. Майже половина (47%) покладаються на паролі, які не змінювали п'ять років.

Для фінансових організацій однією з основних цілей оцифровки є спрощення їх банківських операцій. У спробі поліпшити взаємодію з користувачем однієї з пасток є процес перевірки пароля, необхідного для доступу до мобільного банкінгу. Однак поєднання необхідності підвищення безпеки доступу до облікового запису і прагнення до більшої простоті ускладнює балансування.

Якщо перейти від різних варіантів введення імені користувача і пароля до можливості аутентифікації користувачів по відбитку пальця, це усуне проблему перевантаження з кількістю паролів, які необхідно запам'ятати. Використовуючи біометрію, можна отримати доступ до електронної пошти, онлайн-банку, хмарним сховищам або іншим он-лайн сервісам. Паролем можна поділитися або його вкрасти, але з відбитком пальця все набагато гірше.

Технології відбитків пальців пережили значний бум за останні три роки. В даний час, за оцінками дослідників, близько 31% людей у віці від 18 до 24 років використовують біометричні технології на своїх смартфонах. Однак не є винятком і всі інші користувачі смартфонів, у яких коефіцієнт використання датчика відбитків пальців становить 8%. Дуже ймовірно, що біометрія поширеться і на більш дешеві мобільні телефони.

Поряд з технологією відбитків пальців, великі банки все частіше пропонують клієнтам можливість використовувати голосове керування, сітківку ока та інші біометричні параметри для доступу до своїх рахунків замість паролів. Мета полягає в тому, щоб підвищити безпеку клієнта на додаток до його комфорту. Біометричну аутентифікацію складно імітувати, а клієнтам дуже легко її використовувати. Інноваційні рішення в цій сфері пропонує американська кампанія USAA [2], яка займається наданням банківських послуг, інвестицій, страхуванням і пенсійним обслуговуванням для людей і сімей, які служать або служили в збройних силах Сполучених Штатів. У лютому 2015 року USAA розробила технологію розпізнавання осіб для цілей мобільного банкінгу, а також предоставила голосовий доступ. Це програма, в якій клієнти можуть активувати цю опцію, використовуючи опцію швидкого входу в додаток, і в налаштуваннях вони можуть вибрати розпізнавання обличчя і голоса. Щоб включити функцію розпізнавання голосу, клієнт повинен записати наступну заяву: «Моя особистість захищена, тому що мій голос - це мій пароль. Підтвердіть мене ». Ця заява має бути зроблена в цілому три рази. Потім при реєстрації необхідно чітко і голосно вимовити цю фразу. Розпізнавання облич виконується шляхом фотографування перед реєстрацією. При вході в систему фіксуються підморгування людини, про яку йде мова. Цей аспект допомагає боротися з шахрайством, фотозображення або відео не зможе моргнути в потрібний момент.

USAA також пропонує традиційне розпізнавання відбитків пальців в якості опції для входу в додаток мобільного банкінгу. Таким чином, у клієнтів є кілька варіантів входу в додаток, використовуючи один з кращих біометричних методів: особа, голос, відбиток пальця або введення PIN-коду. На додаток до параметрів безпеки біометричного входу в систему банк також використовує фонову

ідентифікацію пристрою, при якій код, відправлений з пристрою в USAA, зашифрований, а потім порівнюється з зареєстрованим ідентифікатором пристрою.

Одна з найбільш перспективних можливостей нових елементів доступу заснована на авторизації ризиків, т. н. динамічній системі, яка забезпечує доступ в залежності від довіри користувача, що запитує доступ, і конфіденційності інформації, яка захищається. Цей параметр використовує аутентифікацію користувача на основі різних оцінок поведінки користувача з використанням датчиків, таких як камера, акселерометр або GPS. Смартфони можуть збирати широкий спектр інформації про користувачів, включаючи типові вирази обличя, їх звичайну геолокацію, а також те, як він пише, ходить або говорить. Разом ці чинники в 10 разів безпечніше, ніж відбитки пальців і в 100 разів безпечніше, ніж чотиризначні PIN-коди. При такому рівні безпеки телефону користувача вже можна припустити, що людина перед дисплеєм дійсно є тим, хто себе називає.

Використані джерела:

1. Компания TeleSign URL: https://www.linkedin.com/company/telesign
2. Допомога членам USAA URL: https://www.usaa.com/?akredirect=true

Марценюк Л.В.
професор кафедри економіки та менеджменту
Дніпровського національного університету
залізничного транспорту, д.е.н., доцент

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ОНЛАЙН-КУРСІВ ДЛЯ РОЗРОБНИКІВ КОНТЕНТУ

Авторське право – це сукупність правових норм, що регулюють суспільні відносини, які виникають у зв’язку із створенням та використанням творів науки, літератури, мистецтва. Згідно зі ст. 8. Закону України «Про авторське право і суміжні права» «Об’єктами авторського права є твори у галузі науки, літератури і мистецтва, а саме: …виступи, лекції, промови, проповіді та інші усні твори…». Охороні за цим Законом підлягають всі твори, зазначені у частині першій цієї статті, як оприлюднені, так і не оприлюднені, як завершені, так і не завершені, незалежно від їх призначення, жанру, обсягу, мети (освіта, інформація, реклама, пропаганда, розваги тощо) [1].

В контексті бурхливого розвитку дистанційної освіти актуальним стає питання щодо прав на онлайн-курси, які викладач завантажує на тій чи іншій платформі дистанційного навчання, які в подальшому використовуються для навчання студентів. Ці курси можуть належати як автору курсу, так і його замовнику.