3. Роляк А. О. Неперервна професійна освіта: Європейський вимір. *Аграрна наука та освіта в умовах Євроінтеграції*. 2018.

4. Arndt H. W. Economic Development: The History of an Idea. University of Chicago Press, 1989. 217 p.

5. Elsevier B. V. Handbook of Economic Growth, 2014. Vol. 2. 1100 p.

6. Roliak A. Enlightment Stage in the System of Teacher Education of Denmark through Historical Retrospection. *InterConf+*. 2022. № 109. С. 116 - 122.

Олена ПИРЧ
здобувач вищої освіти 4 курсу ОС «бакалавр»
спеціальності 125 «Кібербезпека»,
Хмельницький національний університет,
м. Хмельницький
Науковий керівник: ***Валентина СПІВАЧУК***
кандидат філологічних наук, доцент кафедри іноземних мов,
Хмельницький національний університет,
м. Хмельницький

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ МЕТОДОМ МАСКУВАННЯ

До методів захисту персональної інформації висувається вимога по забезпеченню конфіденційності, навіть при отриманні зловмисником доступу до читання бази даних. Методом, який відповідає даним вимогам є маскування. Маскування – це метод створення структурно подібної, але недостовірної версії даних. Проте існуючі алгоритми маскування не забезпечують достатньої подібності маскованих даних до оригінальних.

Використовуйте маскування даних, щоб приховувати конфіденційні дані, як-от дані кредитних карток, номери соціального страхування або навіть лихослів’я в розмовах. Можна створити правило маскування та визначити регулярний вираз в ньому, щоб визначити конфіденційну

інформацію та замінити її на маскуючий символ. Будь-який замаскований текст у розмові також маскуватиметься в текстовій версії розмови. Маскування даних працює для чату та асинхронних каналів.

Правила маскування можна настроїти таким чином, щоб вони застосовувались до повідомлень, надісланих клієнтом, агентом або обома. Необхідно переконатися, що для правил маскування, які потрібно застосувати, встановлено значення *Активні*, інакше вони не застосовуватимуться до вибраних вами параметрів.

Маскування даних – це спосіб створити фальшиву, але реалістичну версію ваших організаційних даних. Мета полягає в тому, щоб захистити конфіденційні дані, одночасно забезпечуючи функціональну альтернативу, коли реальні дані не потрібні, наприклад, під час навчання користувачів, демонстрацій продажів або тестування програмного забезпечення.

Процеси маскування даних змінюють значення даних під час використання того самого формату. Мета полягає в тому, щоб створити версію, яка не піддається розшифровці або зворотній інженерії. Є кілька способів змінити дані, включаючи перетасування символів, заміну слів або символів і шифрування.

Ось кілька причин, чому маскування даних є важливим для багатьох організацій:

7. Маскування даних вирішує кілька критичних загроз – втрату даних, викрадання даних, внутрішні загрози або компрометацію облікового запису та незахищені інтерфейси зі сторонніми системами.

8. Зменшує ризики даних, пов’язані з використанням хмарних технологій.

9. Робить дані марними для зловмисника, зберігаючи при цьому багато властивих їм функціональних властивостей.

10. Дозволяє обмінюватися даними з авторизованими користувачами, такими як тестувальники та розробники, без розкриття робочих даних.

11. Можна використовувати для дезінфекції даних – звичайне видалення файлу все ще залишає сліди даних на носії даних, тоді як дезінфекція замінює старі значення на замасковані.

Існує кілька типів типів маскування даних, які зазвичай використовуються для захисту конфіденційних даних.

- Статичне маскування даних.

Статичні процеси маскування даних можуть допомогти вам створити очищену копію бази даних. У процесі змінюються всі конфіденційні дані, доки копію бази даних не можна буде безпечно поділитися. Як правило, процес передбачає створення резервної копії бази даних у робочому стані, завантаження її в окреме середовище, видалення будь-яких непотрібних даних і маскування даних, поки вони перебувають у стані. Потім замасковану копію можна перемістити в цільове розташування.

- Детермінізоване маскування даних.

Включає зіставлення двох наборів даних, які мають однаковий тип даних, таким чином, що одне значення завжди замінюється іншим значенням. Наприклад, ім’я «Джон Сміт» завжди замінюється на «Джим Джеймсон», скрізь, де воно з’являється в базі даних. Цей метод зручний для багатьох сценаріїв, але за своєю суттю менш безпечний.

- Маскування даних на льоту.

Маскування даних під час їх передачі з виробничих систем до систем тестування або розробки перед тим, як дані будуть збережені на диску. Організації, які часто розгортають програмне забезпечення, не можуть створити резервну копію вихідної бази даних і застосувати маскування — їм потрібен спосіб безперервної потокової передачі даних із виробництва до кількох тестових середовищ.

На льоту маскування надсилає менші підмножини замаскованих даних, коли це потрібно. Кожна підмножина замаскованих даних зберігається в середовищі розробки/тестування для використання невиробничою системою.

Важливо застосувати маскування на льоту до будь-якого каналу з виробничої системи до середовища розробки на самому початку проекту розробки, щоб запобігти проблемам відповідності та безпеки.

- Динамічне маскування даних.

Подібно до маскування на льоту, але дані ніколи не зберігаються у вторинному сховищі даних у середовищі розробки/тестування. Натомість він передається безпосередньо з робочої системи та споживається іншою системою в середовищі розробки/тестування.

Давайте розглянемо кілька поширених способів маскування конфіденційних даних в організаціях. Захищаючи дані, IT-фахівці можуть використовувати різноманітні методи.

- Шифрування даних.

Коли дані зашифровані, вони стають марними, якщо у засобу перегляду немає ключа дешифрування. По суті, дані маскуються алгоритмом шифрування. Це найбезпечніша форма маскування даних, але її також складно реалізувати, оскільки вона вимагає технології для виконання постійного шифрування даних і механізмів для керування та обміну ключами шифрування.

Персонажі реорганізуються у випадковому порядку, замінюючи оригінальний вміст. Наприклад, ідентифікаційний номер, такий як 76498 у робочій базі даних, можна замінити на 84967 у тестовій базі даних. Цей метод дуже простий у реалізації, але його можна застосувати лише до деяких типів даних і він менш безпечний.

- Обнулення.

Під час перегляду неавторизованим користувачем дані виглядають відсутніми або «нульовими». Це робить дані менш корисними для розробки та тестування.

- Варіація значення.

Вихідні значення даних замінюються функцією, наприклад різницею між найменшим і найвищим значенням у ряді. Наприклад, якщо клієнт придбав кілька продуктів, ціну покупки можна замінити діапазоном між найвищою та найнижчою сплаченою ціною. Це може надати корисні дані для багатьох цілей, не розкриваючи вихідний набір даних.

- Заміна даних.

Значення даних замінюються фальшивими, але реалістичними альтернативними значеннями. Наприклад, справжні імена клієнтів замінюються випадковими іменами з телефонної книги.

- Перетасування даних.

Подібно до підстановки, за винятком того, що значення даних перемикаються в межах одного набору даних. Дані переставляються в кожному стовпці за допомогою випадкової послідовності; наприклад, перемикання між реальними іменами клієнтів у кількох записах клієнтів. Вихідний набір виглядає як реальні дані, але він не відображає справжню інформацію для кожної особи чи запису даних.

- Псевдонімізація.

Відповідно до Загального регламенту захисту даних ЄС (GDPR) було введено новий термін для охоплення таких процесів, як маскування даних, шифрування та хешування для захисту персональних даних: псевдонімізація.

Псевдонімізація, як визначено в GDPR, — це будь-який метод, який гарантує, що дані не можна використовувати для ідентифікації особистості. Це вимагає видалення прямих ідентифікаторів і, бажано, уникнення кількох ідентифікаторів, які в поєднанні можуть ідентифікувати особу.

Підсумовуючи вище сказане, маскування даних — це потужний інструмент, який дозволяє вам точно бачити, як ваші дані виглядають у вашій базі даних, а також може допомогти упевнитися, що немає жодних помилок. Сьогоднішня структура інформаційних потоків, що надсилаються мережею, характеризується ростом відсотку даних, які мають бути захищеними від несанкціонованого доступу. При цьому, останнім часом частішають випадки зламу шифрованих даних, як наслідок морального старіння ряду традиційних методів, зокрема, RSA, так і розширення технічних можливостей зловмисників. За таких умов альтернативою шифруванню можуть виступати технології маскування даних.

Список використаних джерел:

1. Data masking. URL: https://www.imperva.com/learn/data-security/data-masking/

Дарія ПІДДУБНА
здобувач вищої освіти 3 курсу ОС «бакалавр»
спеціальності 014 «Середня освіта.
Мова та література (французька мова)»,
Маріупольський державний університет,
м. Київ
Науковий керівник: ***Марина НЕТРЕБА***
кандидат філологічних наук,
доцент кафедри педагогіки та освіти,
Маріупольський державний університет,
м. Київ

РОЗВИТОК СОЦІАЛЬНО-ЕМОЦІЙНОГО ВИХОВАННЯ В ЗАКЛАДІ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

Соціально-емоційне виховання (СЕВ) – це відносно нова сфера досліджень, яка фокусується на розвитку емоційного інтелекту та соціальних навичок у людей.