УДК 004.4’27:004.77-047.36

Каневський М.В.,

Захарченко С.М.

ОСОБЛИВОСТІ МОНІТОРИНГУ КЛІЄНТСЬКОЇ ЧАСТИНИ В МОБІЛЬНИХ ДОДАТКАХ

Вінницький національний технічний університет, Хмельницьке шосе 98, Вінниця, Вінницька область, 21000

Анотація

У даній роботі представленно проблемі зони моніторингу, який направлений на клієнтську частину мобільних додатків. Виділено особливості взаємодії компанії з користувачем. Також розглянуто юридично сторону взаємодії компанії та клієнта-користувача додатку.

Ключові слова: *моніторинг, GDPR, мобільні додатки*

Abstract

This paper presents the problem of the monitoring area, which is aimed at the client part of mobile applications. The peculiarities of the company's interaction with the user are highlighted. The legal side of the interaction between the company and the client-user of the application is also considered.

Keywords: *monitoring, GDPR, mobile applications*

Вступ

Сучасні мобільні додатки – це не лише взаємодія користувача із самим додатком, а й також його взаємодія з компанією яка цей додаток розробила та підтримує. Важливим фактором для компанії є можливість отримання статистичних даних користувачів додатку, а з боку користувача, впевненість в тому що його конфіденційні дані є захищеними і повідомляються третій стороні.

Задачі

1. Сформувати процесс отримання даних для моніторингу від користувача додатку до компанії розробника
2. Легальність та захищеність даних
3. Способи видалення користувацьких даних

Розв’язання задач

Існує велика кількість систем моніторингу та збирання користувацької інформації, але більшість із них базуються на декількох основних принципах:

1. Збирання основної інформації про користувача (логіни, паролі, геолокація, реквізити, нікнейми, ПІБ, тощо).
2. Шифрування даних за певними алгоритмами.
3. Зберігання даних у шифрованому вигляді строком на 3 роки (країни ЄС та США).
4. Отримання та аналіз інформації про помилки з якими стикається користувач у додатку
5. Можливість увімкнення додаткових логів для користувача або групи користувачів у разі необхідності більш детального аналізу. Немає необхідності робити це для усіх користувачів оскільки велика кількість інформаційних логів дуже швидко завантажує фізичні або віртуальні сервіси збереження даних.

6. Кожна система має свій власний спосіб взаємодії розробника із клієнтською інформацією за допомгою «спілкування» із базою даних[3].
7. Можливість повного видалення клієнтських даних за запитом користувача.

Типовою програмою для збирання такої інформації є Visual Studio App Center від Microsoft. Ця програма дає можливість отримувати звіти про збої які групуються за загальною причиною, виділяючи відповідний кадр стека, щоб можна було знаходити помилки за файлами та або номером рядка, а також шукати збої певних користувачів і переглядайте окремі звіти, щоб знайти хронологію подій та спеціальні вкладення даних[2].

Для легалізації і захисту даних в межах країн ЄС та США було прийнято загальний регламент про захист даних – GDPR — регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Вона також стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам та резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання в межах ЄС.

Регламент замінює Директиву про захист даних і містить положення і вимоги щодо опрацювання особової інформації суб'єктів даних всередині Європейського Союзу. Бізнес-процеси, які опрацьовують персональні дані, повинні бути одразу побудовані за принципом «приватність за призначенням і за замовчуванням», що означає, що персональні дані необхідно зберігати з використанням псевдонімів чи повної анонімізації та використовувати налаштування найвищого рівня приватності за замовчуванням, так щоб дані не були доступні публічно без очевидної згоди та не могли бути використані для ідентифікації суб'єкта без додаткової інформації, що зберігається окремо. Ніякі особисті дані не можуть бути оброблені, якщо це не має під собою законних підстав, визначених регламентом, або якщо контролер чи оператор даних не отримав явної, очевидної згоди від власника даних. Підприємство повинне давати змогу відкликати такий дозвіл у будь-який час.

Контролер персональних даних має чітко заявити, які дані збирає і як, чому їх опрацьовує, як довго зберігає і чи ділиться ними з будь-якими третіми сторонами. Користувачі мають право запросити мобільну копію даних, зібраних оператором, у загальноприйнятому форматі, і право на вилучення їхніх даних за певних обставин. Державні органи, а також підприємства, чия основна діяльність стосується регулярного чи систематичного опрацювання персональних даних, зобов'язані мати посаду співробітника з питань захисту даних (англ. data protection officer, DPO), який стежить за дотриманням GDPR.

Підприємства повинні повідомляти про будь-яке порушення захисту даних, яке має негативний вплив на конфіденційність користувачів, упродовж 72 годин[1].

Важливим аспектом є можливість запиту користувача на повне видалення його даних із системи додатку на стороні компанії-розробника. Цей запит має бути опрацьований впродовж 90 днів після отримання компанією, але компанія розробник залишає за собою право зберігання, лише зберігання і ніяким чином не використання таких даних, впродовж 3 років згідно із деякими законами протидії шахрайству да грального залежності.

Також проблемою є те, що велика кількість компаній-розробників зареєстрована поза межами дії офіційних законів та процедур, а в поєднані з необізнаністю користувачів про їх права та можливості проблема втрати персональних даних є все більш актуальною. Тому ознайомлення користувачем із політикою безпеки, конфіденційності, а також зберіганням та використанням його персональних даних є важливим, в першу чергу із ініціативи самого користувача.

Висновки

Сформовано базові принципи роботи систем зберігання та обробки користувацьких даних.

Розглянуто сопсіб легалізації отримання та зберігання даних компаніями-розбробниками, а також можливості користувачів у видаленні та захисті їх персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Веб ресурс GDPR info https://gdpr-info.eu/
2. Appcenter documentation https://docs.microsoft.com/en-us/appcenter/
3. Library Automation and Monitoring system Jan./Jun. 2018 Costa Rica National University

Відомості про авторів

Каневський Микола Володимирович – аспірант, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: brainiac.kanevskii@gmail.com

Захарченко Сергій Михайлович – кандидат технічних наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет Вінниця, e-mail: zahar@vntu.net

Mykola V. Kanevskyi – Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnitsa, e-mail: brainiac.kanevskii@gmail.com

Sergii M. Zakharchenko – Can. Sc. (Eng.), Assistant Professor of the Computer Techniques Chair, Vinnitsa National Technical University. Vinnitsa, e-mail: zahar@vntu.net