Напрямки та технології захисту персональної інформації

Мірошниченко М.Ю., Таврійський державний агротехнологічний університет імені Дмитра Моторного

Стрімкий розвиток інформаційного суспільства супроводжується повсюдним використанням мережі Інтернет, мобільних застосувань, різноманітних онлайн ресурсів для роботи та відпочинку. Водночас, поряд із значними перевагами, що надає цифровізація суспільства, в інформаційному просторі постійно виникають загрози безпеці даних та інформації, які можуть стати проблемою для звичайних користувачів, державний установ, підприємств та ін. На сьогодні маємо випадки несанкціонованого доступу до персональної інформації, кібератаки, втрати корпоративних даних. Тим самим стає актуальним необхідність в належних заходах захисту для інформаційних систем від внутрішніх та зовнішніх загроз, а також забезпечення безпечної обробки та передачі інформації. Зазначені завдання частіше за все постають перед розробниками програмного забезпечення, системними адміністраторами та фахівцями із захисту інформації. У нашому дослідженні ми висвітлимо основні підходи до захисту інформації та програмного забезпечення від несанкціонованого втручання з боку зловмисників.

Одним з сучасних підходів для захисту акаунтів користувачів є мультифакторна перевірка ідентичності (MFA). Дана технологія заснована на використанні додаткових факторів для ідентифікації користувача, окрім введення логіну та паролю. Тобто, ідентифікація використовує те, що користувач знає (логін та пароль) та який пристрій є в його розпорядженні (мобільний телефон, інший цифровий пристрій). Ця технологія суттєво підвищує рівень безпеки, оскільки навіть у випадку втрати логіну та пароля зловмисники не отримають доступ до акаунту (це може бути соціальна мережа, електронна пошта тощо) без додаткових перевірок. Завдяки цьому технологія захисту MFA є ефективним засобом забезпечення конфіденційності та цілісності даних, протидії несанкціонованому доступу до персональної інформації.

Традиційно для захисту персональних та корпоративних даних використовуються різноманітні методи шифрування, які трансформують дані (зазвичай текстові) за допомогою використання спеціальних ключів. Слід наголосити на декількох особливостях шифрування. Для шифрування даних на рівні додатків використовується симетричне та асиметричне шифрування. В першому випадку ключи використовується для шифрування та розшифрування даних. Асиметричне шифрування передбачає використання двох різних ключів. Ключі повинні зберігатися у захищеному місті. Для безпечного обміну ключами між додатками повинні використовуватися відповідні протоколи.

Досить часто втрата персональної інформації відбувається через злам електронних ресурсів та несанкціоноване отримання доступу до бази даних. Для цього зловмисниками використовуються шкідливі SQL-ін’єкції, які можуть бути виконані через веб-форми, URL-адреси та інші вхідні дані. Для унеможливлення зловмисних дій такого типу застосовується використання параметричних запитів до бази даних, екранування всіх вхідних даних, що надходять від користувачів, застосування правил валідації до вхідних даних. Також доволі часто виникають ситуації втрати персональної інформації внаслідок атак мсжсайтового скриптингу (XSS, Cross-Site Scripting). Для унеможливлення зловмисних дій такого типу застосовується екранування даних, що виводяться на веб-сторінці, використання заголовків безпеки, валідація та фільтрація вхідних даних.

Отже, важливість захисту персональних даних обумовлена можливими критичними наслідками для користувачів. Поряд із зростанням різноманітних атак на комп’ютерні програми та інформаційні ресурси, розвиток технологій вплинув і на розвиток ефективних засобів захисту інформації та програмного забезпечення.