УДК 004.056.53

Дмитро Іванович ЄВСТРАТ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ПРИНЦИПІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПРОЦЕСІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сьогодні далеко не кожен проект може дозволити собі окремого фахівця з безпеки, тому питання реалізації принципів забезпечення кібербезпеки стає предметом особливої уваги не тільки для експертів, а й для звичайних розробників програмного забезпечення. Безпека - це найважливіша характеристика програмного забезпечення, особливо у випадках з системами з програмним управлінням, які можуть вплинути на життя і здоров'я людей, а також системами, які пов'язані з обробкою персональних даних. Безпека програмного забезпечення концептуально відрізняється від функціональних вимог і не настільки зрозуміла інтуїтивно. При цьому, бажана поведінка програми найчастіше сприймається як основна мета, в той час як головна мета безпеки полягає в запобіганні діям, які програма не повинна робити і уникати небажаної її поведінки.

Серед властивостей безпеки програмного забезпечення, існує три основних, відсутності яких необхідно запобігти: конфіденційність, цілісність і доступність. Порушення властивостей безпеки призводить до вразливості програмного забезпечення – пов'язаному з безпекою дефекту, який можна використовувати для досягнення небажаної поведінки.

В процесі розробки безпечного програмного забезпечення необхідно дотримуватися ряду загальних принципів, які можна розділити на наступні групи:

- запобігання (вичерпне усунення дефектів);
- пом'якшення (зменшення шкоди від експлуатації невідомого дефекту);
- виявлення (моніторинг атаки);

— відновлення (нейтралізація шкоди).

На основі цих принципів можна сформулювати рекомендації, яких важливо дотримуватися при розробці, впровадженні і супроводі програмного забезпечення:

— перевага простій архітектурі;
— застосування безпечного вибору за замовчуванням;
— врахування слабкого рівня користувача;
— простий користувальницький інтерфейс;
— обмеження користувача у виборі щодо безпеки;
— використання мінімальної довіреної обчислювальної бази;
— використання відкритих, стандартних для галузі протоколів і алгоритмів;
— максимальне обмеження повноважень для компонентів і користувачів;
— валідація вхідних даних;
— посилення конфіденційності (обмеження доступу до персональних даних);
— розподіл компонентів і операцій;
— об'єднання всіх механізмів безпеки;
— використання стандартних і відкритих рішень;
— збір логів і телеметрії;
— створення резервних копій і знімків стану.

Процес розробки безпечного програмного забезпечення передбачає введення необхідних дій і практик для кожного етапу розробки.

Так, на етапі розробки вимог необхідно визначити:

— вимоги до безпеки;
— необхідні властивості безпеки для компонентів системи;
— механізми безпеки для підтримки цих властивостей;
— моделі загроз.

На етапі розробки:

— визначити архітектуру, з урахуванням загроз безпеки;
— проаналізувати і дати оцінку архітектурним ризикам;

— застосовувати наведені вище принципи безпеки (запобігання, пом'якшення, виявлення, відновлення).

На етапі реалізації:

— дотримуватися кращих практик написання коду;
— проводити обов'язкові рев'ю коду;
— застосовувати інструменти автоматизації для забезпечення високої якості коду.

На етапі тестування проводити:

— тестування на основі ризиків;
— випробування на проникнення;
— навмисне введення в систему випадкових і некоректних даних.

Враховуючи те, що безпека є вторинною характеристикою і часто суперечить функціональності, тому при розробці програмного забезпечення, до якого пред'являються вимоги безпеки, важливим завданням є розробка не просто безпечного, а збалансованого продукту.

Одержано 07.05.2020