Байлюк Є. М., старш. викладач кафедри КІ та КБ,
Россінський Ю. М., канд. техн. наук, доцент кафедри КІ та КБ
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ МОДЕЛЮВАННЯ ЗАГРОЗ

Майже всі інформаційно-комунікаційні системи сьогодні стикають-ся з різними загрозами інформаційної безпеки та кількість цих загроз зростає в міру зміни технологій. Шкідливе програмне забезпечення, яке використовує вразливі місця апаратного та програмного забезпечення, зросло на 51% у другому кварталі 2018 року, а витрати на збитки, спричинені кіберзлочинністю, до 2021 року, відповідно до прогнозів фахівців, сягатимуть 6 трлн. доларів щороку. Загрози можуть надходити як ззовні, так і зсередини організації та можуть мати руйнівні наслідки. Атаки можуть повністю вивести з ладу системи або призвести до витоку конфіденційної інформації, що зменшить довіру споживачів до постачальника системи. Щоб запобігти вдалій реалізації загроз, адміністратори можуть використовувати різні способи та засоби для їх моделювання.

Розглянемо поняття «моделювання загроз». Моделювання загроз – це підхід до проєктування захищених систем, що ґрунтується на оцінці ризику. Він базується на виявленні загроз з метою розроблення пом'якшувальних заходів щодо них. Моделювання загроз слід проводити на початку циклу розробки системи, коли потенційні проблеми можна вия-вити та усунути на ранніх етапах, запобігаючи значним витратам на лік-відацію наслідків атак зловмисників. На даний час існує декілька прог-рамних продуктів для моделювання загроз. Найвідоміші з них – OWASP Threat-Dragon та Microsoft Threat Modeling Tool. Обидва додатки використовують методику STRIDE для побудови моделі загроз.

OWASP Threat-Dragon – це інструмент моделювання загроз з відкритим вихідним кодом від OWASP. Він використовується для створення діаграм моделей загроз, запису можливих загроз та прийняття рішення щодо їх пом'якшення [1]. Приклад побудованої діаграми загроз за допомогою OWASP Threat-Dragon показано на рис.1. Інструмент Microsoft Threat Modeling Tool спрощує моделювання загроз для всіх розробників завдяки стандартній нотації для візуалізації компонентів системи, потоків даних і кордонів безпеки. Це також допомагає розробникам моделей загроз визначати класи загроз, які їм слід враховувати, виходячи зі структури їх інформаційно-комунікаційної системи [2]. Приклад побудованої діаграми загроз за допомогою утиліти Microsoft Threat Modeling Tool показано на рис.2.

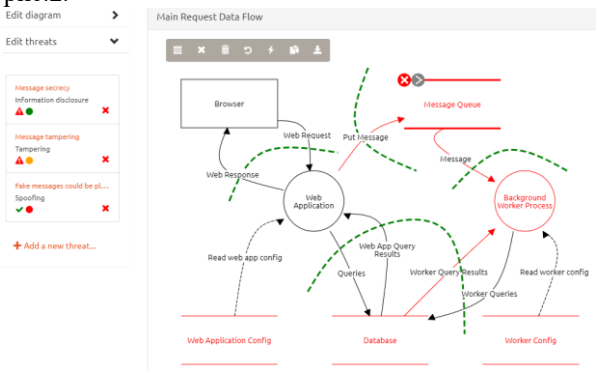

Рис.1. Приклад побудованої діаграми загроз за допомогою програми OWASP Threat Dragon

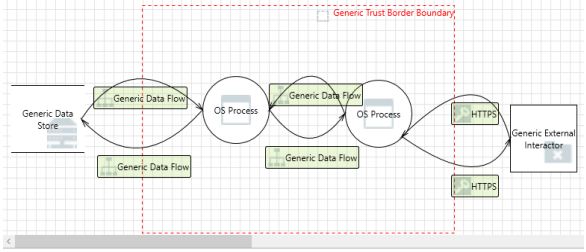

Рис.2. Приклад побудованої діаграми загроз за допомогою утиліти Microsoft Threat Modeling Tool

Таким чином, процес моделювання загроз є одним з основних етапів створення інформаційно-комунікаційних систем. Це дає змогу фахівцям у сфері захисту інформації попередити реалізацію атак зловмисників на ранньому етапі. Для цього вони можуть використовувати різні програмні продукти в залежності від потреб організації.

Список використаних джерел

1. OWASP Threat Dragon. URL: https://owasp.org/www-project-threat-dragon/ (дата звернення 16.11.2020).
2. Threat Modeling. URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling (дата звернення 17.11.2020).