УДК 004.056.5

Б. Ю. Буняк
В. А. Гарнага

Дослідження взаємодоповнюючих підходів: Secure by Design і Zero Trust Architecture

Вінницький національний технічний університет

Анотація

У роботі досліджуються два провідні підходи до забезпечення кібербезпеки: Secure by Design (SbD) та Zero Trust Architecture (ZTA). Проаналізовано їхні основні принципи, сфери застосування і обмеження. Secure by Design розглядається як методологія інтеграції безпеки на всіх етапах життєвого циклу розробки програмного забезпечення (SDLC), тоді як Zero Trust Architecture представлена як стратегічна модель, що базується на принципі «ніколи не довіряй, завжди перевіряй».

Ключові слова: інформаційна безпека, безпека за задумом, архітектура нульової довіри, кібербезпека.

Abstract

This study examines two leading approaches to cybersecurity: Secure by Design (SbD) and Zero Trust Architecture (ZTA). The paper analyzes their core principles, application areas and limitations. Secure by Design is presented as a methodology for integrating security at all stages of the Software Development Life Cycle (SDLC), while Zero Trust Architecture is characterized as a strategic model based on the «never trust, always verify».

Keywords: information security, Secure by Design, Zero Trust Architecture, cybersecurity.

Вступ

Сучасні інформаційні системи функціонують у середовищі, яке зазнає постійних змін – нові загрози, атаки нульового дня, складні ланцюгові проникнення. У такій динаміці традиційні моделі безпеки швидко втрачають свою ефективність. Саме тому на перший план продовжують виходити новітні захисту. Одними із таких стали Secure by Design (SbD) та Zero Trust Architecture (ZTA). У SbD безпека визначається як інтегрована функція на всіх етапах SDLC (Software Development Life Cycle), як заміну традиційному баченню безпеки як «доповнення після розробки». Таким чином відбувається поглиблене загрозоорієнтоване моделювання, де атака може аналізуватися ще до першого рядка коду, яке включає такі принципи безпеки як least privilege, secure defaults і fail-safe mechanisms [1].

Натомість ZTA виступає як модель, що виходить з позиції повної відсутності довіри до будь-якого елементу системи, навіть якщо він є внутрішнім. У даній системі визначається головний принцип: «ніколи не довіряй – завжди перевіряй», задля чого використовується сувора сувора автентифікація, контекстна авторизація і сегментований доступ [2].

Результати дослідження

За останніми стандартами, використання Secure by Design вимагає дотримання ряду технічних підходів: використання бібліотек із безпечним кодом, застосування механізмів типу TEE (Trusted Execution Environment), інтеграцію як статичного, так і динамічного аналізу коду. Використання цих механізмів дозволяє захистити критично важливі обчислення, а також проводити валідацію вхідних даних ще на прикладному рівні. Також важливим є і те, що у SbD розглядається не лише технічна безпека, але і питанням приватності, відповідності стандартам інформаційної безпеки (таким як GDPR, ISO/IEC 27001) [3].

Цікаво, що у концепції SbD жодним чином не ставиться під сумнів внутрішнє середовище – що, як показали інциденти на кшталт атак на SolarWinds (2020), чи Colonial Pipeline (2021), може бути фатальним. Задля вирішення подібних вразливостей, що стосуються внутрішнього середовища, і з’явилася технологія Zero Trust Architecture. У ZTA критичним є саме наявність Policy Engine, який на основі сигналів із Policy Enforcement Point (PEP) і самого алгоритму оцінки довіри ухвалює рішення про надання або відмову в доступі. У даному підході підтримується мікросегментація – ізоляція навіть у мераж одного дата-сервера, де будь-який внутрішній запит перевіряється таким чином, ніби це запит

із зовні. Для прикладу, у хмарній інфраструктурі Microsoft Azure реалізується безперервна оцінка доступу (CAE), що реагує на будь-які зміни у геолокації, сесійні дані, характер запитів у режимі реального часу [4].

Доволі типовим є інтеграція технології ZTA із Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA) та Cloud Access Security Brokers (CASB) – що дозволяє здійснювати швидких заходів у разі виявлення будь-яких аномалій. Проте, слід зауважити, що для розкриття повного потенціалу технології Zero Trust необхідно серйозно перелаштувати мережеву архітектуру, впровадити складні IAM-механізми, що безсумнівно спричинить низку незручностей для організацій через складність та вартість впровадження необхідних змін [5].

Тож, що технологія ZTA, що SbD були створенні для мінімізації ризиків, проте використовуються на різних рівнях: Secure by Design – на етапі створення, у той час як Zero Trust Architecture – у процесі експлуатації. І закономірно випливає, що у випадку поєднання цих технологій буде отримана система із безпечним дизайном, де кожен компонент – ізольований, верифікований і мінімально привілейований, а із зовні все контролюється Zero Trust-політикою, що забезпечила б адаптивний контроль у режимі реального часу. Таке поєднання максимально підвищила б безпеку відповідно до сучасних потреб.

Висновки

Було розглянуто дві сучасні стратегії забезпечення кібербезпеки – Secure by Design (SbD) та Zero Trust Architecture (ZTA). SoD орієнтується на запобігання вразливостям ще на етапі проєктування ПЗ – шляхом інтеграції принципів мінімальних привілеїв, безпечних налаштувань за замовчуванням і багаторівневої валідації. Натомість ZTA повністю відмовляється від довіри до будь-яких елементів системи, навіть внутрішніх, та впроваджує перевірку кожного запиту через політики доступу, автентифікацію та аналіз контексту.

Обидва підходи мають свої особливості. SbD працює ще до запуску системи, тоді як ZTA забезпечує контроль у реальному часі під час її використання. Їх поєднання дозволяє створити цілісну модель захисту – від безпечного коду до контрольованого доступу. За даними NIST та CISA, таке поєднання відповідає найкращим сучасним практикам [2, 5]. Додатково, провідні компанії, як-от Microsoft та IBM, вже проваджують обидва підходи у свої хмарні сервіси, що свідчить про їхню ефективність у реальному застосуванні [4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. NIST SP 800-160 (2020). *Інженерія системної безпеки: багатодисциплінарний підхід до створення надійних захищених систем*. URL: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final
2. NIST SP 800-207 (2020). *Архітектура нульової довіри (Zero Trust Architecture)*. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final
3. ISO/IEC 27001:2022 *Інформаційна безпека, кібербезпека та захист приватності — Системи менеджменту інформаційної безпеки — Вимоги*.
4. Документація з безпеки Microsoft Azure (2023). *Безперервна оцінка доступу в Azure AD (Continuous Access Evaluation in Azure AD)*. URL: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation
5. Центри безпеки в Інтернеті (CISA) (2023). Модель зрілості нульової довіри. URL: https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model (дата звернення 01.06.2025)

Буняк Богдан Ю. – студент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: bbuniak@ukr.net

Гарнага Володимир А. – кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: garnaga.volodymyr@vntu.edu.ua

Buniak Bohdan Y. – student of the Department of Information Security, Vinnytsia NationalTechnical University, Vinnytsia, e-mail: bbuniak@ukr.net

Harnaha Volodymyr A. – PhD, Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: garnaga.volodymyr@vntu.edu.ua