УДК 004.77:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.166

АРХІТЕКТУРУ БЕЗПЕКИ "НУЛЬОВОЇ ДОВІРИ"

Усов О.О.
Науковий керівник – Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. IMI, м. Харків, Україна
e-mail: oleksandr.usov@nure.ua

Zero Trust is one of the latest cybersecurity buzzwords. Therefore, it is important to understand what Zero Trust is – and what Zero Trust is not. Zero Trust is a strategic initiative that helps prevent data leaks by eliminating the concept of trustworthiness from an organization's network architecture. The basic principle is “don’t believe anything without checking.” Zero Trust protects modern digital environments by leveraging network segmentation, preventing threat propagation, providing application-level threat defense, and simplifying granular access control for users.

Архітектура безпеки "нульової довіри" (Zero Trust Security Architecture) - це політика безпеки, яка полягає в тому, що жодна частина мережі або окремий користувач не повинні мати довіри до жодного об’єкту або суб’єкту мережі без перевірки. Тобто цей підхід базується на принципі "ніколи не довіряй, завжди перевіряй". Замість традиційного периметру безпеки, в якому внутрішній мережевий трафік вважається довіреним, у архітектурі "нульової довіри" кожен запит на доступ до ресурсів або сервісів обробляється і перевіряється.

Ця архітектура передбачає, що кожен запит на доступ до ресурсу або послуги повинен бути автентифікований, авторизований та обмежений за необхідності. Навіть користувачі, які знаходяться всередині мережі, повинні проходити через той самий процес перевірки, як і зовнішні користувачі. Основні принципи архітектури "нульової довіри" включають мінімізацію дозволів доступу, мікросегментацію мережі, багаторівневу автентифікацію та авторизацію, шифрування даних у спокійному стані та в руху, а також неперервний моніторинг та аналіз активності.

Переваги «нульової довіри»:

1. Зменшує ризик несанкціонованого доступу до ресурсів.
2. Знижує ризик витоків і розкриття даних у разі порушення безпеки.
3. Підвищує гнучкість: дозволяє безпечно надавати доступ до ресурсів користувачам, які працюють віддалено або з мобільних пристроїв.
4. Спрощує управління: централізує управління доступом до ресурсів.

Впровадження нульової довіри - це складний процес, який потребує

ретельного планування та виконання.

Безперервне підтвердження справжності учасників суб'єктів і об'єктів інформаційного доступу – постійна автентифікація та авторизацію з урахуванням усіх доступних точок доступу даних, підсилена ідентифікація пристрої та розмежування прав доступу користувачів

Налаштування доступу з мінімальними правами – обмеження доступу користувачів за часом і обсягом прав, застосування адаптивної політики безпеки, яка ґрунтується на основі оцінювання інформаційних ризиків; застосування апаратно-програмних засобів захисту, які не впливають на продуктивність мережі.

Розгляд кожного запиту на роботу в мережі як порушення безпеки - зменшення радіусу можливої атаки та обмеження доступу до сегментів інфокомунікаційної мережі; застосування наскрізного шифрування.

Незважаючи на багатоцілісні переваги, архітектура "нульової довіри" може зустрітися з певними викликами та обмеженнями. Наприклад, її впровадження може вимагати значних витрат на час та ресурси, а також технічний експертизи. Крім того, необхідно забезпечити сумісність з існуючими інфокомунікаційними системами та процесами, що може бути складно в деяких випадках.

Однак не зважаючи на ці виклики, архітектура "нульової довіри" залишається однією з найефективніших стратегій захисту інформації в інфокомунікаціях, яка забезпечує надійний захист від кіберзагроз та захистити дані від розкриття та модифікаціїтам .

Список використаних джерел:

1. Was ist eine Zero-Trust-Architektur? [Електронний ресурс] // The Forrester Wave™: Privileged Identity Management. – 2018. – Режим доступу до ресурсу: https://www.paloaltonetworks.de/cyberpedia/what-is-a-zero-trust-architecture.

2. Zero Trust Architecture [Електронний ресурс] / S.Rose, O. Borchert, S. Mitchell, S. Connelly // NIST Special Publication. – 2020. – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.SP.800-207.

3. Zero Trust Architecture / [C. Green-Ortiz, B. Fowler, D. Houck та ін.]. – Singapore: O\'Reilly, 2023. – 336 с. – (Cisco Press).