Рудюк Б. М., магістрант,
Єфіменко А. А., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ZTNA ТА ZTNA 2.0

У сучасному цифровому середовищі, коли безмежні потоки корпоративних даних циркулюють у віртуальному просторі, для будь-якої компанії питання безпеки виходить на перший план. Забезпечення конфіденційності та цілісності інформації стає надзвичайно важливим завданням у контексті стрімкого зростання кіберзагроз. Традиційні методи захисту, такі як VPN, не завжди спроможні протистояти новим викликам, що зумовлює необхідність впровадження інноваційних підходів, таких як доступ до мережі з нульовою довірою (ZTNA, ZeroTrustNetwork Access).

ZTNA – це сукупність технологій, яка забезпечує безпечний віддалений доступ до програм і служб на основі визначених політик контролю доступу.

ZTNA грунтується на трьох основних принципах:

1. Не довіряти нікому.
2. Перевіряти все.
3. Надавати доступ лише до того, що потрібно

Системи, які будуються на базі ZTNA, не довіряють жодному користувачеві, пристроєві чи мережі незалежно від їх розташування. Такі системи виконують перевірку всіх спроб доступу до ресурсів, незалежно від того, звідки надходять запити. Системи надають доступ користувачам лише до тих ресурсів, які їм потрібні для виконання їхніх завдань.

При використанні ZTNA, доступ до конкретних програм або ресурсів надається лише після автентифікації користувача у службі ZTNA. Після успішної автентифікації ZTNA створює захищений шифрований тунель для користувача, через який надається доступ до визначеної програми. Цей тунель забезпечує додатковий рівень захисту, захищаючи програми та служби від виявлення за їх IP-адресами, які в іншому випадку могли б бути доступні.

ZeroTrustNetwork Access 2.0 (ZTNA 2.0) вирішує проблеми, що випливають з застарілих рішень ZTNA, забезпечуючи надійне з’єднання для компаній з гібридними робочими потоками. Його основна мета – забезпечити безпечний доступ до ресурсів, зберігаючи при цьому високий рівень зручності користування.

ZTNA 2.0 порівняно з ZTNA 1.0 забезпечує:

- мінімізацію привілеїв доступу;
- постійну перевірку довіри;
- постійну перевірку безпеки;
- загальну безпеку даних;
- захист для всіх додатків.

За допомогою ідентифікації програм на 7-му рівні моделі OSI можна точно контролювати доступ на рівні окремих додатків і їх компонентів, незалежно від інших мережевих параметрів, таких як IP-адреси і номери портів. Після отримання доступу, рівень довіри постійно переоцінюється на основі змін у поведінці пристрою, користувачів та додатків. Також постійно проводиться глибока перевірка всього трафіку, включаючи дозволені з'єднання та захист від усіх видів загроз, включаючи загрози нульового дня. Використовуючи єдину політику DLP, дане рішення забезпечує послідовний контроль даних у всіх корпоративних додатках, включаючи приватні програми та SaaS. ZTNA 2.0 забезпечує захист всіх корпоративних додатків, включаючи хмарні, застарілі приватні та SaaS, включаючи програми, що використовують динамічні порти або посилання, ініційовані сервером.

ZTNA 2.0 може бути складнішою у впровадженні та управлінні і може бути дорожчою, ніж ZTNA, через необхідність додаткових інструментів та функцій.

Таким чином, ZTNA та ZTNA 2.0 є ефективними стратегіями безпеки, які дозволяють мінімізувати ризики кібератак та забезпечують безпеку мережі на сучасному рівні. Хоча обидва підходи мають свої переваги, ZTNA 2.0 видається більш привабливим варіантом завдяки своїм покращеним функціональним можливостям та здатності до інтеграції з іншими технологіями безпеки. Однак вибір між ними повинен залежати від конкретних потреб та умов кожної організації.

Список використаних джерел

1. John Wiley & Sons Inc. ZTNA For Dummies. Palo Alto Networks Special Edition, 2022. 52 p.
2. What Is Zero Trust Network Access (ZTNA). Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna