

БЕЗПЕКА «НУЛЬОВОЇ ДОВІРИ»

Традиційні стратегії забезпечення безпеки не працюють, і все більше компаній стають жертвами зловмисників. За даними опитування, проведеного компанією PricewaterhouseCoopers (PwC) [1], загальна кількість інцидентів у сфері безпеки по всьому світу зростає.

Мета даної роботи полягає в проведенні всебічного аналізу існуючих методів розмежування доступу до ресурсів комп'ютерних систем на прикладі моделі безпеки «нульової довіри».

Сьогодні основні джерела кіберзагроз – це іноземні держави, конкуренти і організована злочинність. За даними PwC, кіберзлочинці поступово переключаються на середній бізнес, так як великі підприємства посилюють захист.

Багато підприємств досі використовують застарілі технології (наприклад, мережі VPN і брандмауери периметра мережі), розроблені задовго до появи сучасних способів злому.

Модель «нульової довіри» розмежовує окремі мережні компоненти, щоб надійно захистити найважливіші дані, запобігти несанкціонованому доступу до них з боку додатків і користувачів, посилити безпеку вразливих систем і виключити проникнення в мережу шкідливих програм.

Мережа «нульової довіри» побудована на п'яти основних твердженнях [3]:

- мережа завжди вважається ворожою.
- зовнішні та внутрішні загрози завжди існують у мережі.
- локальна мережа недостатня для вирішення довіри до мережі.
- кожен пристрій, користувач і мережний потік автентифікований і авторизований.
- політика повинна бути динамічною та обчислюватися з якомога більшої кількості джерел даних.

В основі моделі «нульової довіри» лежить принцип «Не довіряй і перевіряй»: жоден об'єкт, незалежно від його типу, розташування або приналежності до корпоративної мережі, що не вважається безпечним. Такий підхід допоможе запобігти атакам кіберзлочинці та інших зловмисників.

З моделлю «нульової довіри» не існує довіри за замовчуванням для будь-якої організації - включаючи користувачів, пристроїв, додатків і пакетів - незалежно від того, що вона є та її місцезнаходження на або відносно

корпоративної мережі. Встановивши межі «нульової довіри», які ефективно розділяють різні сегменти мережі, можна захистити критичну інтелектуальну власність від несанкціонованих додатків або користувачів, зменшити вплив вразливих систем і запобігти бічному переміщенню шкідливих програм у вашій мережі.

Мережі «нульової довіри» не вимагають нових протоколів або бібліотек. Проте вони використовують існуючі технології новими способами. Системи автоматизації дозволяють створювати та експлуатувати мережу нульової довіри [2].

Існує багато способів реалізації цієї автоматизації. Цілеспрямовані системи є найбільш ідеальними, хоча тут також можуть поміститися більш звичайні системи, такі як традиційне керування конфігураціями. Широке впровадження управління конфігураціями є важливим етапом для нульової мережі довіри, оскільки ці системи часто підтримують запаси пристроїв і здатні автоматизувати конфігурацію мережного нагляду у площині даних.

Аналіз даної теми показав, що при побудові архітектури розробники забувають, що далеко не всі компоненти корпоративної мережі є надійними. Крім того, немає належного рівня прозорості, контролю і захисту вхідного і вихідного трафіку.

Відзначимо, що модель «нульової довіри» не пов'язана з конкретними постачальниками і має гнучку архітектуру, що враховує індивідуальні вимоги до безпеки.

Організації, що використовують модель «нульової довіри», будуть використовувати її як можливість для повторного вивчення своєї політики і процесів в області кібербезпеки. Вони також все частіше звертаються до провайдерів керованих послуг безпеки, щоб розширити свої можливості моніторингу та управління безпекою. Це дозволить їм зосередитися на отриманні максимальної віддачі від своїх інвестицій в засоби контролю безпеки і ресурси, а також забезпечити їх належне та ефективне застосування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Managing cyber risks in an interconnected world [Електронний ресурс]. Режим доступу: <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.
2. Top IT trends in 2018: cybersecurity [Електронний ресурс]. Режим доступу: <https://www.dimensiondata.com/it-trends/cybersecurity-2018>
3. Chapter 1. Zero Trust Fundamentals [Електронний ресурс]. Режим доступу: <https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html>.