УДК 004.7

Гладченко О.В., к.пед.н., доцент
Луценко Н. О., здобувачка
Державний податковий університет

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ В УМОВАХ СУЧАСНИХ РИЗИКІВ

Стрімкий розвиток інформаційно-комунікаційних технологій зумовив фундаментальну трансформацію корпоративних мережевих інфраструктур і суттєво змінив підходи до забезпечення їхньої безпеки. Якщо на попередніх етапах розвитку інформаційних систем мережі підприємств характеризувалися чітко визначеним фізичним і логічним периметром, централізованою архітектурою та обмеженим набором сервісів, то сучасні корпоративні середовища функціонують у складній розподіленій екосистемі. Така екосистема включає використання публічних і приватних хмарних платформ, сервісів віддаленого доступу, мобільних і персональних пристроїв, а також інтеграцію з інформаційними ресурсами партнерських організацій і сторонніх провайдерів послуг. Унаслідок цього традиційні межі мережевого периметра стають умовними, а контроль над потоками даних ускладнюється. Розширення поверхні атаки підвищує ймовірність компрометації інформаційних активів, що вимагає перегляду підходів до побудови систем кіберзахисту.

На ранніх етапах розвитку мережевих технологій основні кіберзагрози були пов'язані з експлуатацією відкритих мережевих портів і базових служб, що забезпечували передачу даних та віддалене керування системами. Зловмисники виконували сканування діапазонів IP-адрес для визначення активних вузлів, після чого здійснювали детальний аналіз відкритих сервісів, версій операційних систем і прикладного програмного забезпечення [1, с. 28–29]. Такий підхід дозволяв формувати карту мережевої інфраструктури та виявляти потенційні точки входу. Найбільш поширеними інструментами атак у цей період були використання відомих вразливостей системного та мережевого програмного забезпечення, реалізація атак типу DoS і DDoS з метою порушення доступності сервісів [2, с. 124], а також перебір облікових даних користувачів через слабкі механізми автентифікації. Відповідно до таких загроз основним засобом захисту виступали міжмережеві екрани, які здійснювали фільтрацію мережевого трафіку за IP-адресами джерела та призначення, номерами портів і типами транспортних протоколів.

З розвитком вебтехнологій та переходом бізнес-процесів у цифрове середовище вектори атак зазнали суттєвих змін. Зловмисники почали активно використовувати вразливості прикладного рівня, що сприяло поширенню складних атак на вебзастосунки. Серед найбільш небезпечних методів можна виокремити SQL-ін'єкції, які дозволяють отримувати несанкціонований доступ до баз даних, міжсайтовий скриптинг, спрямований на виконання шкідливого коду в браузері користувача, а також атаки на механізми керування сесіями та автентифікації. Особливість таких загроз полягає в тому, що мережевий трафік, який використовується для їх реалізації, часто передається через дозволені порти та стандартні протоколи HTTP або HTTPS. У результаті шкідлива активність маскується під легітимні запити, що значно ускладнює її виявлення традиційними засобами мережевого захисту, орієнтованими переважно на аналіз мережевого рівня.

Крім того, сучасні вебзастосунки характеризуються складною багаторівневою архітектурою, використанням API-інтерфейсів, мікросервісних підходів та інтеграцією з хмарними сервісами. Це створює додаткові вектори потенційних атак і підвищує вимоги до засобів моніторингу та контролю мережевого трафіку. Таким чином, еволюція інформаційних технологій спричинила необхідність переходу від статичних моделей периметрового захисту до адаптивних багаторівневих систем кібербезпеки, здатних враховувати прикладний контекст, поведінкові характеристики мережевих з'єднань і динамічні зміни середовища функціонування корпоративних мереж. Наступним етапом розвитку кіберзагроз стало поширення цільових довготривалих атак, які характеризуються ретельною підготовкою, використанням соціальної інженерії та здатністю зловмисника тривалий час залишатися непоміченим у системі. Додаткові труднощі створює широке застосування протоколів шифрування TLS, що призводить до формування «сліпих зон» у процесі моніторингу мережевого трафіку.

Традиційна модель мережевої безпеки базувалася на концепції периметрового захисту, відповідно до якої внутрішня мережа вважалася довіреним середовищем [3]. Проте сучасні кіберзагрози продемонстрували обмеженість такого підходу. Зокрема, класичні міжмережеві екрани не здатні виконувати глибокий аналіз прикладного контексту трафіку, що дозволяє шкідливим запитам маскуватися під легітимні HTTPS-з'єднання.

Важливою проблемою є також наявність внутрішніх загроз, пов'язаних із компрометацією робочих станцій, діяльністю інсайдерів або неконтрольованим поширенням шкідливого програмного забезпечення між сегментами мережі. За відсутності логічної

сегментації навіть одиничне проникнення може призвести до масштабної компрометації всієї інфраструктури.

Суттєвим недоліком традиційних систем безпеки є відсутність механізмів кореляції подій та інтелектуального аналізу аномалій у режимі реального часу. Це ускладнює виявлення багатоступеневих атак, у межах яких зловмисник поступово розширює свої привілеї та здійснює горизонтальне переміщення мережею. Крім того, використання розрізнених інструментів безпеки — від IDS-систем до автономних VPN-шлюзів — призводить до технологічної фрагментації, що ускладнює адміністрування та підвищує ризик помилок конфігурації.

У відповідь на стрімке ускладнення ландшафту кіберзагроз та зростання масштабів цифровізації корпоративних середовищ сформувалася концепція багаторівневого захисту, яка передбачає впровадження комплексу взаємопов’язаних механізмів контролю на різних рівнях функціонування інформаційної системи [4]. Основною метою такого підходу є створення послідовної системи бар’єрів безпеки, де компрометація одного компонента не призводить до автоматичного доступу до інших сегментів інфраструктури. Реалізація багаторівневого захисту дозволяє підвищити стійкість корпоративних мереж до зовнішніх та внутрішніх загроз, забезпечуючи ефективну локалізацію інцидентів та мінімізацію потенційних збитків.

Одним із ключових елементів цієї концепції є логічна сегментація мережевого середовища. Поділ інфраструктури на ізольовані функціональні зони за допомогою технологій віртуальних локальних мереж, створення віртуальних інтерфейсів та впровадження гранулярних міжсегментних політик доступу дозволяє значно обмежити можливості горизонтального переміщення зловмисника.

Важливу роль у сучасних системах кіберзахисту відіграють технології глибокої інспекції пакетів, які забезпечують аналіз мережевого трафіку не лише на рівні заголовків пакетів, а й з урахуванням прикладного контексту переданих даних [5]. Це дозволяє ідентифікувати шкідливу активність, замасковану під легітимні мережеві запити, зокрема використання небезпечних скриптів, спроби несанкціонованого доступу до вебресурсів або передачу шкідливих вкладень. Використання механізмів DPI у поєднанні з системами запобігання вторгненням, контролю застосунків і вебфільтрації створює комплексний підхід до аналізу мережевих подій у режимі реального часу.

Подальший розвиток підходів до забезпечення мережевої безпеки пов’язаний із впровадженням концепції нульової довіри, яка передбачає

безперервну перевірку користувачів, пристроїв і сервісів незалежно від їх фізичного або логічного розташування [6]. У межах цієї моделі відсутнє поняття «довіреної внутрішньої мережі», а кожна мережева взаємодія розглядається як потенційно небезпечна. Доступ до інформаційних ресурсів надається відповідно до принципу мінімальних привілеїв із урахуванням контекстних параметрів, таких як рівень захищеності пристрою, поведінкові характеристики користувача, місцезнаходження, час запиту та тип виконуваної операції. У поєднанні з багаторівневими механізмами контролю, централізованими системами моніторингу та автоматизованими інструментами реагування це дозволяє сформувати адаптивну архітектуру кіберзахисту, здатну ефективно протидіяти складним сучасним кібератакам.

Список використаних джерел

1. Тарнавський Ю.А. Технології захисту інформації. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с. URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua

2. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ: Київський столичний університет імені Бориса Грінченка, 2018. 320 с. URL: https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf

3. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підруч. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236с. URL: https://ftp.kr-labs.com.ua/books/kozura-zahyst-info-v-komp-systemah.pdf

4. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підруч. Київ: Видавництво НА СБ України, 2020. 256 с. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf

5. Терейковський І.А., Гнатюк С.О. Захист інформації в комп'ютерних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2022. 135 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/0dbba7ac-40e4-4a83-80b7-f729109cfe9a/content

6. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. URL: https://doi.org/10.6028/NIST.SP.800-207