Ульяніцький М. А., магістрант,
Бродський Ю. Б., к.т.н.,доцент
Державний університет «Житомирська політехніка»

ПІДСИСТЕМА ЗАХИСТУ КЛІЄНТ-СЕРВЕРНОЇ МЕРЕЖІ ВІД КІБЕРАТАК

Кібератаки можуть виникнути в будь-який момент і на будь-якій інфраструктурі, тому питання кібербезпеки є надзвичайно важливим.

Підсистема захисту клієнт серверної мережі від атак на Active Directory є дуже актуальною в сучасному світі інформаційних технологій. Active Directory є одним з основних компонентів сучасних корпоративних мереж, і важливо забезпечити його захист від різного роду атак, таких як злом паролів, використання недійсних логінів і багато інших. До складу Active Directory входить кілька різних служб. Основною службою є служби домену, але Active Directory також включає служби полегшених каталогів (AD LDS), протокол доступу до спрощених каталогів (LDAP), служби сертифікатів або AD CS, служби федерації (AD FS) і служби керування правами (AD RMS). Різні команди працюють по всій Україні, і люди можуть підключатися до незахищених мереж, що робить їхні дані доступними для зловмисників.

Головна мета дослідження полягає в аналізі, розробці та впровадженні ефективної підсистеми захисту клієнт-серверної мережі з метою запобігання кібератак.

Мета дослідження реалізована на основі використання передових технологій та методів захисту, зокрема впровадження сучасних систем виявлення вторгнень, застосування шифрування даних, використання механізмів аутентифікації та авторизації, а також моніторингу та реагування на інциденти безпеки в реальному часі.

Захист клієнт-серверних мереж від кібератак є надзвичайно важливим завданням у сучасному цифровому світі. Для забезпечення безпеки таких мереж використовуються різноманітні технології та методи:

- Firewalls та Інтрузійна Детекція/Запобігання (IDS/IPS): Захищають мережу від несанкціонованого доступу та виявляють аномалії для запобігання атак;
- шифрування Даних та VPN: Забезпечують конфіденційність інформації та захищають передачу даних через зашифровані канали;
- сегментація мережі та політики безпеки: розділяє мережу для обмеження поширення атак та встановлення правил безпеки;
- антивірусне ПЗ та оновлення безпеки: захищають від вірусів та забезпечують встановлення патчів для закриття вразливостей.

Ці технології та методи становлять ключову підсистему захисту клієнт-серверних мереж від різноманітних кібератак.

Аналіз загроз у сфері кіберзахисту клієнт-серверних мереж полягає у виявленні потенційних атак та вразливостей, що можуть бути використані для несанкціонованого доступу до даних чи систем. Технічні рішення для захисту таких мереж включають в себе методи захисту, такі як застосування брандмауерів, впровадження систем виявлення вторгнень (IDS) та запобігання вторгнень (IPS), шифрування даних, регулярне оновлення програмного забезпечення, використання сегментації мережі, резервне копіювання даних, антивірусні заходи та навчання персоналу щодо кібербезпеки. Ці заходи спрямовані на попередження атак та зменшення можливості їхнього успішного впровадження, що дозволяє забезпечити більш високий рівень безпеки в клієнт-серверних мережах.

Інноваційні підходи до кіберзахисту клієнт-серверних мереж включають застосування штучного інтелекту та машинного навчання для розпізнавання аномальної активності та передбачення потенційних загроз. Техніки аналізу поведінки користувачів та систем в реальному часі дозволяють виявляти неочікувані відхилення та швидко реагувати на кіберзагрози.

Отже, кібератаки стають все більшою загрозою для організацій та інфраструктури, особливо в умовах сучасних конфліктів. Забезпечення кіберзахисту та розробка підсистем захисту для клієнт-серверних мереж є невід'ємною складовою в умовах постійно зростаючих кіберзагроз. Аналіз загроз та застосування технологій захисту, таких як шифрування, мережеві брандмауери, системи виявлення вторгнень та інші, демонструють необхідність постійного вдосконалення та адаптації заходів безпеки до нових викликів кіберпростору. Тому, лише комплексний, системний підхід та поєднання різноманітних технологій та методів захисту можуть забезпечити ефективний захист клієнт-серверних мереж від сучасних кібератак.

Список використаних джерел

1. Active Directory. URL: https://www.cyberark.com/what-is/active-directory/