УДК 004.056(477)

Андрій ПЕКАР, Сергій ВОЗНЯК

Західноукраїнський національний університет

МЕТОДИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОРПОРАТИВНИХ МЕРЕЖАХ

Вступ. У сучасному світі інформаційних технологій забезпечення безпеки корпоративних мереж стає все більш важливим завданням. У зв'язку зі зростанням числа кібератак і витоків даних організаціям необхідно приділяти особливу увагу захисту своєї мережевої інфраструктури. Несанкціонований доступ до корпоративних ресурсів може призвести до серйозних наслідків, таких як фінансові втрати, втрата конфіденційної інформації та репутаційний ризик. Новітні методи виявлення та запобігання несанкціонованому доступу постійно вдосконалюються для протидії новим загрозам та забезпечення надійного захисту корпоративних активів.

Мета: вивчити і проаналізувати новітні методи виявлення і запобігання несанкціонованого доступу в корпоративних мережах, щоб визначити їх ефективність і можливості застосування в реальних ситуаціях. Розгляньте комплексний підхід до мережевої безпеки, що включає технічні, організаційні та програмні засоби захисту. У ньому викладаються основні тенденції розвитку систем безпеки і даються рекомендації з побудови ефективної системи безпеки корпоративної мережі.

1. Огляд методів виявлення та моніторингу аномальної активності в мережі

У зв'язку зі стрімким розвитком інформаційних технологій і зростанням кіберзагроз проблема виявлення і моніторингу аномальної активності в мережі стає все більш актуальною [1].

Сучасні методи аналізу мережевого трафіку та виявлення аномалій засновані на передових алгоритмах машинного навчання та статистичного аналізу, які дозволяють ефективно виявляти потенційні загрози та запобігати несанкціонованому доступу до мережевих ресурсів [2].

Статистичні методи аналізу мережевого трафіку є одним з найбільш поширених підходів до виявлення аномалій. Вони засновані на припущенні, що нормальна робота мережі може характеризуватися певними статистичними показниками, а відхилення від неї можуть вказувати на наявність аномальної активності. Методи статистичного аналізу можуть бути використані для досягнення високої ефективності при виявленні мережевих атак та аномальної поведінки [3].

На рисунку 1 показано порівняння ефективності різних статистичних методів виявлення аномалій на основі експериментальних даних.

Рисунок 1 - Архітектура системи моніторингу мережевої активності

Важливим аспектом ефективного моніторингу мережевої активності є правильне налаштування та конфігурація системи виявлення аномалій. За даними одного з досліджень [4], оптимальне налаштування порогових значень і параметрів аналізу може значно підвищити ефективність виявлення аномалій і зменшити кількість помилкових спрацьовувань. Особливу увагу слід звернути на вибір метрик і показників, які використовуються для оцінки нормальної поведінки мережі.

Сучасні тенденції розвитку методів виявлення аномалій включають використання штучного інтелекту та технологій великих даних. Використання розподілених систем обробки даних та хмарних технологій може значно підвищити масштабованість та ефективність систем моніторингу. Іншим важливим напрямком розвитку є інтеграція різних джерел даних для створення інтегрованої системи аналізу безпеки.

Аналіз методів виявлення та моніторингу аномальної активності в мережах показує, що найбільш ефективним підходом є поєднання різних методів аналізу та використання адаптивних алгоритмів, які можуть навчатися на минулих даних. За даними одного з досліджень [5], такий підхід дозволяє досягти точності виявлення аномалій понад 90% при прийнятному рівні хибних спрацьовувань.

На особливу увагу заслуговує захист об'єктів критичної інфраструктури та систем управління технологічними процесами. Згідно з дослідженням [6], традиційні методи виявлення аномалій можуть бути неефективними в таких системах через особливості мережевого трафіку та протоколів зв'язку. Необхідна розробка спеціальних методів аналізу, що враховують особливості промислових мереж та систем управління.

Іншим важливим аспектом є забезпечення відповідності систем моніторингу законодавчим вимогам та галузевим стандартам безпеки. Сучасні системи виявлення аномалій повинні не тільки надавати можливість аудиту та документування всіх виявлених інцидентів, а й реагувати на загрози відповідно до встановлених процедур механізмами, що потребують підтримки.

Перспективними напрямками розвитку методів виявлення аномалій є використання квантових обчислень та технології блокчейн. Згідно з дослідженнями [7], квантові алгоритми можуть значно підвищити ефективність аналізу складних мережевих структур та виявлення прихованих залежностей у даних. Технологія блокчейн може забезпечити надійне зберігання та верифікацію даних про виявлені інциденти.

2. Інструменти та технології для запобігання несанкціонованому доступу

Системи виявлення та запобігання вторгнень (IDS/IPS) залишаються одним з ключових елементів захисту мережевої інфраструктури [8]. Сучасні IDS/IPS використовують поєднання сигнатурного аналізу та методів машинного навчання для виявлення потенційних загроз. Особлива увага приділяється їх здатності виявляти нові типи атак і аномальну поведінку в мережі; інтеграція IDS/IPS з іншими системами безпеки дозволяє створити єдиний центр моніторингу та реагування на інциденти [9].

Міжмережеві екрани нового покоління (NGFW) забезпечують розширені можливості фільтрації мережевого трафіку та контролю доступу. На відміну від традиційних брандмауерів, NGFW можуть аналізувати трафік на рівні додатків, виявляти шкідливе програмне забезпечення та захищати від новітніх загроз; важливою особливістю NGFW є те, що вони можуть інтегруватися з системами управління безпекою та автоматизувати процес реагування на інциденти.

Важливу роль в управлінні доступом до ресурсів компанії відіграють системи управління ідентифікацією та доступом (IAM). Сучасні IAM-рішення підтримують багатофакторну автентифікацію, єдиний вхід (SSO) та управління правами користувачів.

На рисунку 2 показано типову архітектуру IAM-системи та її взаємодію з іншими компонентами інфраструктури безпеки.

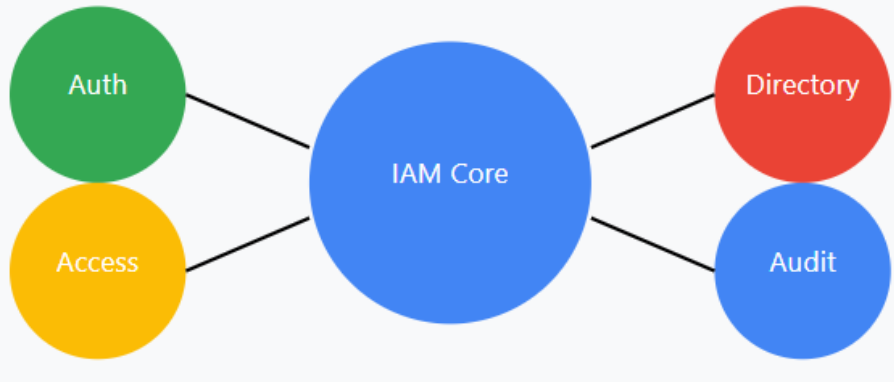

Рисунок 2 - Архітектура системи IAM

Ключовим компонентом будь-якої сучасної системи безпеки є рішення для виявлення та реагування на загрози на кінцевих точках (EDR). Ці інструменти безперервно відстежують активність на робочих станціях і серверах, виявляють підозрілу поведінку і автоматично реагують на інциденти; рішення EDR інтегруються з центральними системами управління безпекою для забезпечення розширених можливостей розслідування інцидентів.

Шифрування даних залишається одним з основних механізмів захисту конфіденційної інформації. Сучасні рішення для шифрування підтримують різноманітні алгоритми та протоколи, що гарантують захист даних як при зберіганні, так і при передачі. Особлива увага приділяється управлінню ключами та дотриманню нормативних вимог.

Технології віртуалізації та контейнеризації ставлять нові виклики перед системами безпеки. Захист віртуальних середовищ вимагає спеціальних інструментів і підходів, таких як мікросегментація мережі та захист контейнерів. Важливим аспектом є забезпечення безпеки в гібридних і мультихмарних середовищах.

Штучний інтелект і машинне навчання все частіше використовуються в системах безпеки для автоматизації виявлення загроз і реагування на інциденти. Ці технології дозволяють аналізувати великі обсяги даних і виявляти складні патерни атак. Особлива увага приділяється розробці адаптивних систем безпеки, здатних навчатися на нових загрозах.

Висновок. Виявлення та запобігання несанкціонованому доступу в корпоративних мережах є першочерговим завданням для забезпечення

інформаційної безпеки. У нашій статті було проведено детальне дослідження сучасних методів виявлення та моніторингу аномальної активності в мережі, які демонструють різноманітність підходів і інструментів, що використовуються для виявлення підозрілих дій.

Аналіз показав, що системи виявлення та запобігання вторгненням (IPS), у поєднанні з багатофакторною автентифікацією (MFA), суттєво підвищують рівень безпеки. Системи IPS ефективно виявляють загрози на рівні мережі, а MFA надає додатковий рівень захисту на етапі аутентифікації користувачів, що є критично важливим у контексті сучасних ризиків, пов'язаних з віддаленим доступом і інсайдерською загрозою.

Окремо ми зосередились на новомодних технологіях, таких як алгоритми машинного навчання та штучного інтелекту, які показують значний потенціал у автоматизації процесу виявлення аномалій. Дослідження вказують на те, що ці технології здатні не тільки швидше ідентифікувати підозрілі активності, але і адаптуватися до змінюваних патернів поведінки зловмисників.

Проте, жоден метод не забезпечує абсолютної гарантії захисту. Це підкреслює важливість мультидисциплінарного підходу до безпеки, який включає не лише технологічні рішення, а й освіту співробітників, актуалізацію політик безпеки та регулярні аудити.

Наше дослідження також вказує на необхідність гнучкості та адаптації підходів до кібербезпеки відповідно до еволюційних загроз, оскільки кіберзлочинці постійно вдосконалюють свої методи. Лише через інтеграцію багатьох технологій і постійне вдосконалення стратегій можна забезпечити надійний захист інформаційних активів корпоративних мереж у сучасному динамічному середовищі.

Перелік використаних джерел.

1. Al-Shaer, E., Hamed, H. Modeling and Verification of IPsec and VPN Security Policies. International Journal of Information Security, 2023.

2. Vasilenko, N., Miroshnychenko, O. Security Monitoring Systems in Corporate Networks. Cyber Security Journal, 2024.

3. Barros, M., Stein, L. Advanced Intrusion Detection Techniques in Corporate Networks. IEEE Transactions on Network Security, 2023.

4. Anderson, R., Moore, T. The Economics of Information Security. Science, 2023.

5. Tanase, M. Understanding and Preventing Unauthorized Network Access. Packet Labs Network Security Review, 2022.

6. Chen, Y., Fang, H. Multi-Layered Defense Strategies for Enterprise Security. Journal of Network Defense, 2022.

7. Altman, R. Role-Based Access Control Mechanisms for Corporate Network Security. Information Security Journal, 2022.

8. Smith, J. Intrusion Prevention and Detection Systems in Corporate Environments. Cybersecurity World, 2023.

9. Ikeda, R. Using AI and Machine Learning for Threat Detection. IT Security Journal, 2024.