УДК 004.49

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ АТАК

Барцицький Андрій, студент групи 1ПЗ-16м,
Рейда Олександр , доцент кафедри програмного забезпечення,
Вінницький національний технічний університет

Вступ

З появою нових інформаційних технологій з'являються і нові загрози, які пов'язані з можливими атаками зловмисників. Забезпечення високого рівня безпеки і захисту від інформаційних атак є однією з найбільш актуальних проблем, що пов’язана з постійним вдосконаленням засобів захисту і виявленням атак. Тому актуальним є аналіз можливостей захисту від інформаційних атак та перспектив розвитку систем інформаційної безпеки.

Об’єктом дослідження постають технології захисту від інформаційних атак. Предметом дослідження є системи захисту і виявлення інформаційних атак.

Основною задачею роботи є аналіз перспектив розвитку систем виявлення інформаційних атак з метою забезпечення високої надійності системи інформаційної безпеки.

Результати дослідження

Інформаційна атака – це сукупність дій зловмисника, спрямована на порушення конфіденційності, цілісності або доступності інформації.

Для виявлення таких атак існують спеціальні системи. Системами виявлення інформаційних атак (СВІА) називають сукупність програмних і апаратних засобів, які в разі виявлення будь-яких підозрілих або просто нетипових подій, здатні робити самостійні дії по виявленню, ідентифікації і усуненню їх причин [1].

СВІА є базовим елементом загальної системи інформаційної безпеки. На кожні 100 інформаційних атак сьогодні створюється нова система, що дозволяє виявити і запобігти цим атакам [2].

Отже, розглянемо можливі тенденції розвитку СВІА за напрямками, в яких перспективним є їх подальший розвиток.

1. Очевидно, що незабаром будемо спостерігати нові технології в області збору інформації в СВІА. По-перше, це створення власних механізмів в СВІА збору інформації, що дозволить забезпечити їх незалежність від засобів аудиту зовнішніх додатків, а також дозволить отримати додаткову інформацію, наприклад, при клавіатурному введенні користувача, і оцінити характер роботи запущених додатків. По-друге, це збільшення швидкості обробки мережевого трафіку. Уже сьогодні розробляють стандарт, який буде забезпечувати швидкість 100 Гб / с [3]. По-третє, розвиток методів обробки та кореляції даних, що збираються.

2. Створення більш ефективних поведінкових методів виявлення інформаційних атак, які за ефективністю не поступатимуться сигнатурним методам. Це дозволить підвищити ймовірність виявлення нових загроз і недопущення помилок в процесі роботи СВІА.

3. Орієнтація на атаки внутрішніх зловмисників. Ведуться розробки СВІА, орієнтовані на внутрішні загрози. У перспективі очікується створення систем з високим рівнем захисту від несанкціонованих дій користувачів.

4. Використання багатоядерного підходу в системах виявлення атак. Актуальність багатоядерного захисту від вірусів обумовлена тим, що працездатність антивірусних ядер різних виробників відрізняється часом реагування на ті чи інші віруси, тож пріоритетним завданням є досягнення максимально швидкої реакції на вірус за допомогою багатоядерного підходу, що поєднує компоненти різних виробників.

5. Використання багатоагентної архітектури. Під агентами розуміються комп'ютерні системи, що функціонують в складному динамічному середовищі і виконують певні функції. Перевагами такого підходу є: масштабованість, можливість зниження навантаження на мережу, можливість використання декількох СВІА в рамках єдиної платформи, висока продуктивність роботи, підвищення відмовостійкості.

6. Уніфікація мови опису сигнатур інформаційних атак. Це дозволило б в одній СВІА використовувати сигнатури інших виробників, підвищуючи якість випущених сигнатур. Так, наприклад, в даний час вже кілька виробників комерційних систем використовують мову системи "Snort".

7. Інтеграція з іншими засобами захисту. Можливим варіантом інтеграції буде програмний комплекс захисту, який буде виконувати функції виявлення атак, антивірусу, засобів захисту від спаму, засобів тематичного аналізу, а також брандмауера.

8. Спрощення процесу первинного налаштування СВІА. Залежно від конфігурації СВІА її налаштування може тривати від декількох днів до декількох тижнів. Перспективною є задача створення дієвих механізмів, орієнтованих на автоматизацію і прискорення процесу налаштування системи.

Висновки

Розвиток систем виявлення інформаційних атак акумулює комплексний підхід багатоагентної архетектури з використанням багатоядерного підходу, орієнтацією як на зовнішнього, так і на внутрішнього зловмисника, уніфікацією мови опису сигнатур інформаційних атак з метою забезпечення високої продуктивності та надійності роботи системи та спрощення процесу її налаштування.

Список використаної літератури

1. ICCM / Системи виявлення вторгнень. [Електронний ресурс]. Режим доступу: http://www.icmm.ru/~masich/win/lexion/ids/ids.html.
2. Системи виявлення атак. [Електронний ресурс]. Режим доступу: http://www.bytemag.ru/articles/detail.php?ID=6608
3. Нове в захисті від злому корпоративних систем Техносфера, 2007. - 360 с. - 3000 прим. - ISBN 978-5094836-133-8