УДК 004.738.5:004.056

Левошко О.Л.
Центральноукраїнський національний технічний університет

Комплексні системи захисту інформаційних систем

Захист інформаційної системи дає найкращі результати, якщо до нього підходити комплексно. Комплексна система захисту включає в себе захист об'єктів інформаційної системи, захист каналів зв'язку, процесів, програм і процедур обробки інформації, управління системою захисту, захист інформаційних мереж. В даний час захист інформації є важливою частиною інформаційних систем і в останні роки розвивається дуже добре. Воно й зрозуміло, адже чим далі, тим більше ми приходимо до розуміння, що найцінніший ресурс - це інформація, і вона теж потребує захисту. Головний напрямок пошуку нових шляхів захисту інформації полягає не просто у створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, використовувані для захисту інформації, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також нештатних ситуацій технічного характеру. Для мінімізації ризиків інформаційної безпеки в інформаційних мережах в наш час актуальним є комплексний підхід для виявлення мережевих атак. Цей підхід включає в себе розробку та впровадження систем виявлення мережевих атак. Вони представляють собою спеціалізовані програмні або програмно-апаратні засоби, які дозволяють здійснювати активний аудит та управління безпекою (прогнозувати, виявляти, попереджувати, контролювати, реагувати в реальному масштабі часу на ризики безпеки) в мережі. Розв'язання задач для здійснення ефективного захисту інформації від мережевих атак вимагає розробки нових методів, які спроможні протидіяти розподіленим мережевим атакам різного походження та більш адекватно відображати складну динаміку випадкових процесів цих атак. Потрібна розробка методів виявлення розподілених мережевих атак, які використовують комплексні сучасні методи підтримки прийняття рішень на основі теорії інтелектуальних систем, що дозволяють здійснювати перехід від процесів виявлення і ліквідації до процесів прогнозування та попередження в реальному масштабі часу. Розрізняють декілька методів виявлення мережевих атак:

- виявлення атак зловмисної поведінки;
- виявлення атак аномальної активності;
- багатоагентні системи виявлення аномальної мережевої активності.

Технологія виявлення атак зловмисної поведінки базується на виявленні атаки, яка потребує розуміння очікуваної поведінки порушника інформації, який підлягає контролю. Робота систем виявлення зловживань ґрунтується на складанні шаблонів. Захисні системи цього типу мають ефективність на відомих схемах атак, однак у випадку нової невідомої атаки або відхилення від шаблону, виникають проблеми. При цьому необхідно постійно підтримувати та оновлювати велику базу даних, яка включає не тільки атаки та її варіації, та безперервно поповнювати бази шаблонів. Крім цього, важливо правильно визначати об'єм вибірки параметрів, які контролюються методом виявлення

мережевої атаки, яка базується на зловмисній поведінці. Технологія виявлення мережевих атак, яка базується на методах виявлення аномальної активності, відрізняється від розглянутої вище. Вона більш гнучка та дозволяє виявляти невідомі атаки. Системи виявлення аномалій ґрунтуються на припущенні, що всі дії зловмисника обов'язково відрізняються від поведінки звичайного користувача, тобто його дії вважаються аномальними. Виявлення атак обумовленні аномальною активністю та основані на порівнянні поточних значень параметрів активності , значення яких на даний момент визнані нормальними. Дана технологія базується на тому, що аномальна поведінка суб'єкта (системи, програми, користувача), проявляється як відхилення від нормальної поведінки. Ця технологія вимагає постійної реєстрації всіх дій об'єкту, що контролюється, яка необхідна для виявлення аномальної активності. Враховуючи перспективи розвитку систем інформаційних технологій, а також об'єктивні недоліки, описаних попередньо двох комплексних підходів виявлення мережевих атак, можна зробити висновок про необхідність розробки та впровадження комплексних методів побудови систем захисту, які базуються на розподілених обчислювальних системах та з використанням механізмів захисту на основі активного аудиту. Складові компоненти таких систем повинні бути спеціалізовані по типам задач, що необхідно розв'язувати, взаємодіяти один з одним з метою обміну інформацією та прийняття злагоджених рішень, адаптуватися до реконфігурації апаратного та програмного забезпечення мережі, зміни трафіку, новим видам атак та їх варіацій. Серед можливих технологій реалізації такого комплексного підходу, який є найбільш перспективним, вважається технологія інтелектуальних багатоагентних систем. Дана технологія полягає в наступному: компоненти системи захисту інформації (агенти захисту) являють собою інтелектуальні автономні програми, які реалізовують визначені функції захисту з метою забезпечення необхідного класу захисту. Вони дозволяють реалізувати комплексну надбудову над механізмами безпеки мережевих програмних засобів, операційних систем та додатків, які використовуються, при цьому підвищуючи захист системи до необхідного рівня. Виконання процесу прогнозування та виявлення розподілених мережевих атак – є ключовим фактором специфічних функцій багатоагентної системи виявлення мережевих атак. Виявлення мережевих атак на ресурси систем інформаційних технологій – дуже складний технологічний процес, який пов'язаний зі збором великої кількості інформації про функціонування систем інформаційних технологій, аналізом цього об'єму даних та виявлення факту атаки. Для ефективного прогнозування та виявлення атак необхідне комплексне застосування різних методів виявлення мережевих атак. Цей підхід об'єднує в собі метод багатоагентних систем та метод адекватного виявлення ознак атак на основі статистичних методів теорії ймовірностей, нечітких статистичних методів, методів теорії інтелектуальних систем та методів штучних нейронних мереж. При злагодженій реалізації даних методів в системі виявлення мережевих атак, можна досягти в широкому діапазоні умов функціонування мереж.

Список використаних джерел

1. *Земцов, Ю.В. Комплексный подход к обнаружению сетевых атак [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/doc/zemcov.doc*
2. *Биячуев, Т.А. Безопасность корпоративных сетей / под ред. Л.Г. Осовецкого. – СПб ГУ ИТМО, 2004 – 161с.*
3. *Девянин, П.Н. Модели безопасности компьютерных систем: Учебн. пос. для студ. ВУЗ / П.Н. Девянин – М.: изд. Центр «Академия», 2005.- 144с.*
4. *Завгородний, В.И. Комплексная защита информации в компьютерных системах: Учебн. Пос.– М.: Логос; ПБОЮЛ Егоров Н.А., 2001. - 264с.*