УДК 004.056.53

О.В. Сєвєрінов, А.Г. Хрєнов

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

У статті розглянуто види сучасних систем виявлення вторгнень, що забезпечують захист інформаційних систем та мереж. Проведено аналіз алгоритмів захисту та на його основі виявлено основні переваги та недоліки кожного виду.

Ключові слова: *аналіз сучасних систем виявлення вторгнень, системи виявлення вторгнень, захист інформаційних систем та мереж, види систем виявлення вторгнень.*

Вступ

В даний час зростання ролі інформаційних систем у сфері військового управління призводить до посилення загроз використання проти інтересів України кібернетичних засобів як зсередини держави, так і з-за кордону.

На теперішній час можливості систем виявлення вторгнень є необхідним критерієм щодо інфраструктури захисту інформації [1] в системах управління з'єднань та частин ЗС України, які використовують інформаційні системи з підключенням до глобальної мережі Інтернет. Згідно аналізу центра скарг Інтернет-злочинності за 2013 рік, взагалі було отримано 262 813 скарги про вторгнення до інформаційних мереж від користувачів та організацій з втратами на суму у розмірі 781 841 611$ [2].

На рис. 1 зображено графік зростання атак на інформаційні системи та мережі за останні роки. З аналізу вищенаведеної статистики витікає, що система безпеки даних є критичною складовою в повсякденній діяльності з'єднань та частин ЗС України.

Під час інтеграції системи виявлення вторгнень у мережу певного з'єднання або частини ЗС України виникає питання вибору виду такої системи виявлення. Кожна частина ЗС України має індивідуальну архітектуру мережі, що вимагає від відповідальної служби робити обґрунтований вибір системи виявлення вторгнень через їх велику вартість та ймовірні комбінації при інтеграції.

Метою статті є аналіз та порівняння різних видів систем виявлення вторгнень в інформаційних системах та мережах.

Системи виявлення вторгнень

Система виявлення вторгнень (СВВ, IDS – Intrusion Detection System) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу [3]. Системи виявлення вторгнень забезпечують виявлення:

- мережеві атаки проти вразливих сервісів;
- атаки спрямовані на підвищення прав користувачів;
- неавторизований доступ до важливих файлів;
- дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

Використання СВВ допомагає досягнути такі цілі:

- виявити вторгнення або мережеві атаки;
- забезпечити належний контроль якості адміністрування, особливо у великих і складних мережах;
- спрогнозувати можливі майбутні атаки і виявити вразливості для запобігання їх подальшого розвитку;
- отримати корисну інформацію про проникнення, для відновлення і налаштування конфігурації мережі;
- визначити розташування джерела атаки по відношенню до локальної мережі (зовнішні або внутрішні атаки).

Архітектура СВВ

На рис. 2 зображена архітектура типових систем виявлення вторгнень.

Рис. 1. Графік зростання атак на інформаційні системи та мережі за останні роки

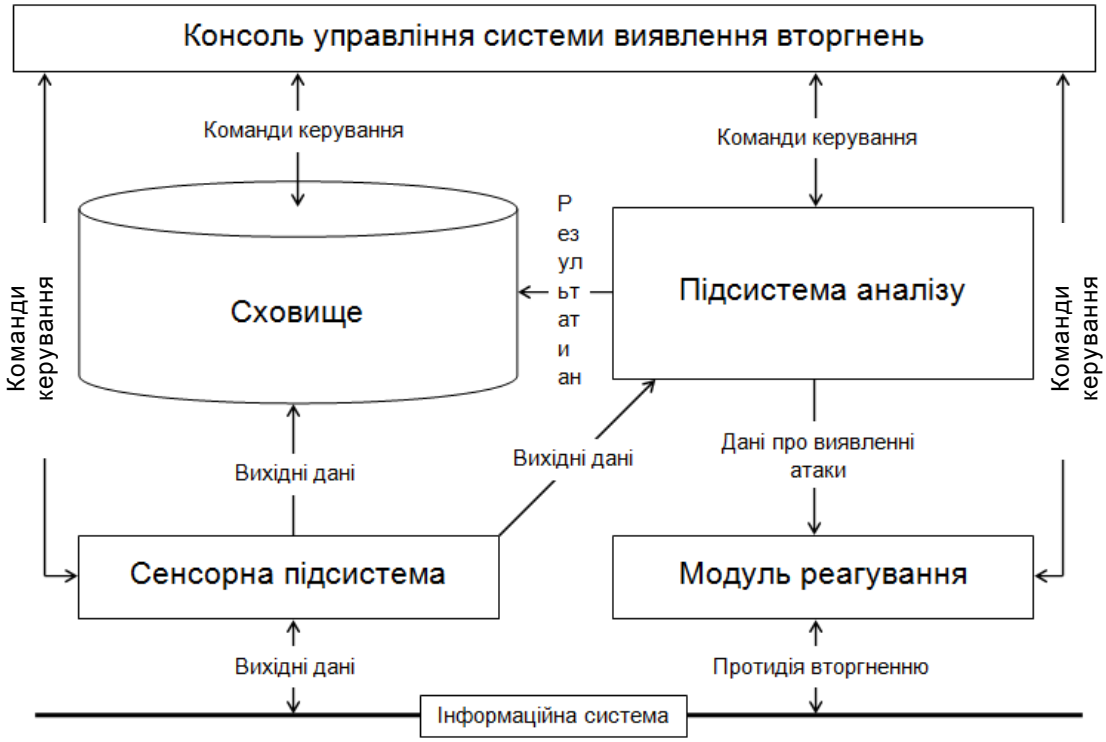

Рис. 2. Архітектура типових систем виявлення вторгнень

Основними компонентами систем виявлення вторгнень є сенсорна підсистема, підсистема аналізу, сховище, консоль управління та модуль реагування.

Сенсорна підсистема, призначена для збору подій, пов'язаних з безпекою мережі або системи, що захищається.

Підсистема аналізу, призначена для виявлення мережевих атак і підозрілих дій.

Сховище, в якому накопичується база первинних подій і результати аналізу.

Консоль управління, що дозволяє конфігурувати СВВ, спостерігати за станом мережі або інформаційної системи та СВВ, переглядати виявлені підсистемою аналізу інциденти несанкціонованих вторгнень.

Модуль реагування, який встановлений в системах активної протидії відповідає за виконання інструкцій по протидії несанкціонованому вторгненню в мережу або систему.

Види систем виявлення вторгнень

На сьогоднішній день існує кілька різних типів СВВ систем, що відрізняються різними алгоритмами моніторингу даних і підходами до їх аналізу. Кожному виду системи відповідають ті чи інші особливості використання, переваги і недоліки.

Один із методів класифікації СВВ систем ґрунтується на з'ясуванні того, як вони проводять мониторинг інформаційної системи або мережі. Одні контролюють весь мережевий трафік і аналізують мережеві пакети, інші розгортаються на окремих комп'ютерах і контролюють операційну систему на предмет виявлення ознак вторгнення.

За способами моніторингу СВВ системи підрозділяються на network-based (NIDS) і host-based (HIDS).

NIDS (network-based) визначають атаки, захоплюючи і аналізуючи мережеві пакети. Слухаючи мережевий сегмент, NIDS може переглядати мережевий трафік від кількох хостів, які приєднані до мережевого сегменту, і таким чином захищати ці хости.

Зважаючи на особливості розташування таких систем виявлення можна виділити такі переваги:

- не впливають на продуктивність існуючої інформаційної системи;
- велике покриття для моніторингу та у зв'язку з цим централізоване управління;
- такі СВВ, як правило, пасивні пристрої, які перехоплюють мережевий трафік, не навантажуючи мережу службовими потоками.

Але на фоні важливих переваг такого виду систем виявлення вторгнень спостерігаються наступні недоліки:

- не здатні аналізувати зашифровану інформацію;
- повідомляють про ініційований напад, не аналізуючи ступінь проникнення;
- не в змозі розпізнавати напад в момент високого навантаження інформаційної системи;
- не можуть розпізнати результат атаки. NIDS не можуть сказати чи була атака успішної, вони

можуть тільки визначити, що атака була почата. Це означає, що після того як NIDS визначить атаку, адміністратор повинен вручну досліджувати кожен атакований хост для визначення, чи відбувалося реальне проникнення;

- вимагають додаткового налаштування і функціональності мережевих пристроїв;

HIDS (host-based) мають справу з інформацією, що збирається всередині єдиного комп'ютера. Таке вигідне розташування дозволяє HIDS аналізувати діяльність з великою вірогідністю і точністю, визначаючи тільки ті процеси і користувачів, які мають відношення до конкретного вторгнення в операційну систему інформаційної мережі. HIDS зазвичай використовують інформаційні джерела двох типів: результати аудиту операційної системи і системні логи.

За рахунок вигідного розташування безпосередньо на сервері, такий вид систем виявлення вторгнень має значні переваги:

- не вимагають додаткової функціональності мережевих пристроїв;
- мають можливість стежити за подіями локально щодо хоста, можуть визначати атаки, які не можуть бачити NIDS;
- працюють в мережі, що використовує шифровані дані, коли інформація знаходиться в відкритому вигляді на сервері до її відправки клієнту;

Але через особливості роботи операційної системи, місце розташування систем виявлення та методи вторгнень можна спостерігати наступні недоліки:

- механізми збору інформації повинні встановлюватися і підтримуватися на кожному сервері, який буде контролюватися;
- можуть бути атаковані і заблоковані підготовленим супротивником;
- не здатні контролювати ситуацію у всій мережі, так як «бачать» тільки мережеві пакети, одержувані сервером, на якому вони встановлені;
- використовують обчислювальні ресурси сервера, який контролюють, знижуючи тим самим ефективність його роботи;

Висновки

Отже, враховуючі всі особливості систем виявлення вторгнень та детально ознайомившись з недоліками та перевагами обох видів даних систем можна прийти до висновку, що найкращим захистом для інформаційної системи з'єднання або частини ЗС України буде гібридне використання одночасно обох видів систем IDS у одній інформаційній мережі.

Такий метод дозволить надійно захистити інформаційну систему використовуючи всі переваги систем виявлення вторгнень. Але варто пам'ятати, що системи IDS це лише один з інструментів захисного арсеналу і він не повинен розглядатися як заміна для будь-якого з інших захисних механізмів. Захист інформації найбільш ефективний, коли в мережі підтримується багаторівневий захист.

Список літератури

1. Многоагентные технологии комплексной защиты информации в телекоммуникационных системах / В.И. Городецкий, И.В. Котенко, О.В. Карсаев, А.В. Хабаров // Труды 7-й межд. конф. по информационным сетям и системам ISINAS – 2000 (октябрь).– СПб., 2000. – С. 122-134.

2. Сайт http://netconfig.ru/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: http://netconfig.ru/server/ids-ips/.

3. Сайт www.ic3.gov [Електронний ресурс]. – Режим доступу до матеріалу сайту: http:// www.ic3.gov/media/IC3-Poster.pdf.

4. Сайт http://ru.wikipedia.org/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: http://ru.wikipedia.org/wiki/Система_обнаружения_вторжений.

Надійшла до редколегії 26.05.2014

Рецензент: д-р техн. наук, ст. наук. співр. О.О. Можаєв, Харківський національний технічний університет «ХПІ», Харків.

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

О.В. Сєвєрінов, А.Г. Хрєнов

У даній статті розглянуто види сучасних систем виявлення вторгнень, що забезпечують захист інформаційних систем та мереж. Проведено аналіз алгоритмів захисту та на основі аналізу алгоритмів виявлено основні переваги та недоліки кожного виду.

Ключові слова: *аналіз сучасних систем виявлення вторгнень, системи виявлення вторгнень, захист інформаційних систем та мереж, види систем виявлення вторгнень.*

ANALYSIS OF MODERN INTRUSION DETECTION SYSTEMS

A.V. Severinov, A.G. Khrenov

This article discusses the types of modern intrusion detection systems, which protect information systems and networks. Through the analysis of algorithms intrusion detection systems, we have identified the advantages and disadvantages of their use.

Keywords: *analysis of current intrusion detection systems, intrusion detection systems, protection of in-formational systems and networks, types of intrusion detection systems.*