УДК 621.396

М. В. Васильківський
О. В. Стальченко
О. В. Ремінський

ІНФОРМАЦІЙНА ЗАХИЩЕННІСТЬ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація

Досліджено способи підвищення інформаційної захищеності корпоративних програмних систем зв'язку. Проведено аналіз методів, використовуваних в системах штучного інтелекту (ШІ) і можливостей їх застосування для оцінки захищеності програмних систем (ПС).

Ключові слова: корпоративна інформаційна система, корпоративна програмна система, штучний інтелект.

Annotation

The ways of increasing the information security of corporate software communication systems are investigated. The analysis of the methods used in artificial intelligence (AI) systems and the possibilities of their application to assess the security of software systems (PS).

Keywords: corporate information system, corporate software system, artificial intelligence

ВСТУП

Сучасне суспільство не уявляє своє існування без програмних систем (ПС), в тому числі і складних систем автоматизації виробництва, управління польотами, управління електростанціями та без корпоративних інформаційних систем (КІС), що забезпечують обробку великих обсягів інформації.

Якість КІС та корпоративних програмних систем (КПС) безпосередньо впливає на ефективність роботи підприємств і організацій, а одним з показників якості КПС є їх захищеність. Забезпечення захисту ускладнюється тим, що не можна формально описати та передбачити дії зловмисника. Постійний розвиток і зростання складності КПС є ще одним фактором, що впливає на їх захищеність. Дуже важливим стає завдання створення еталонів для оцінки поточної захищеності КПС, які враховують нові вразливості і погрози. Такі еталони безпеки можна було б застосовувати як при розробці нових систем, так і для оцінки захищеності вже функціонуючих систем. Завдання отримання таких еталонів є слабо формалізовано і для його вирішення потрібен детальний аналіз безлічі параметрів систем.

На сьогоднішній день однією з найбільш перспективних областей для проведення досліджень є область штучного інтелекту (ШІ). На даний момент активно ведуться дослідження в галузі ШІ, результати яких успішно впроваджуються в різні сфери людської діяльності. Тому перспективним напрямком досліджень є застосування систем ШІ для вирішення завдань контролю безпеки (КБ) ПС. Вже є кілька прикладів успішного використання продукційних систем [1], нейронних мереж [2], багатоантенних систем [3] для вирішення завдань КБ.

Метою даної роботи є підвищення ефективності засобів оцінки захищеності корпоративних програмних систем на основі статичних та динамічних еталонів безпеки.

Результати досліджень

Засоби аналізу захищеності (ЗАЗ) призначені для виявлення вразливих місць з метою їх оперативної ліквідації. Самі по собі вони ні від чого не захищають, але допомагають виявити, а деякі і усунути, проблеми в захисті раніше, ніж їх зможе використовувати зловмисник. В основному ЗАЗ спрямовані на помилки адміністрування, тобто на помилки конфігурації використовуваного програмного і апаратного забезпечення, і на неуважність обслуговуючого персоналу до виходу нових версій, які «закривають» відомі вразливості. Ці засоби не розглядають архітектурні проломи, так як їх складно, а іноді і неможливо усунути.

ЗАЗ також називаються сканерами захищеності (або безпеки). Дані засоби засновані на накопиченні і використанні знань про проблеми в захисті: про те, як їх шукати, наскільки вони серйозні і як їх усувати. Ядро таких систем - це база вразливих місць, яка містить відомі ЗАЗ вразливості, і, тим самим, визначає її можливості. База вразливостей вимагає практично постійного оновлення.

Основними механізмами сканерів для перевірки є сканування і зондування [4]. Першим механізмом є пасивний. Використовуючи сканування, сканер намагається виявити вразливості, але не підтверджує їх. Він аналізує непрямі ознаки. Такий метод перевірки найбільш швидкий і простий в реалізації. Компанія ISS такий підхід називає «логічний кінець». Компанія Cisco описує сканування, як пошук відкритих портів на всіх мережевих пристроях і збір пов'язаних з портами заголовків. Всі зібрані заголовки перевіряються по базі правил, в якій містяться мережеві пристрої, операційні системи та потенційно вразливі місця. В результаті перевірки робиться висновок про те, чи присутні вразливості на сканованих пристроях.

Другий механізм є активним. Зондування використовує засоби імітації атак для того, щоб підтвердити наявність вразливостей. Цей метод працює повільніше, але більш точно, тому що результат його роботи не «здогад» про наявність вразливості, а результат проведення атаки. Компанії ISS називає цей варіант перевірки «підтвердженням». Cisco має на увазі під зондуванням використання інформації, отриманої на етапі сканування, для більш детального аналізу кожної вразливості. Варто зауважити, що цей метод може використовувати відомі реалізації атак. Це буває необхідно, щоб підтвердити вразливості, які неможливо виявити пасивними методами. Наприклад, вразливості типу «відмова в обслуговуванні».

На практиці сканування реалізується двома методами: перевірка заголовків і активні зондувальні перевірки.

Перевірка заголовків полягає в надсиланні запиту про перевірку ПС і аналізі отриманої відповіді. Наприклад, це може бути спроба отримати версію встановленого модуля PHP і припущення про наявність в ньому вразливостей, які присутні в стандартній конфігурації цієї версії. Перевірка заголовків є найшвидшим і простішим в реалізації методом, але у нього є ряд істотних недоліків. По-перше, він може бути непридатний, тому що рекомендацією до забезпечення безпеки компанії є приховування детальної інформації про використаний ПЗ, і відповідь на перевірку може просто не містити необхідні для перевірки дані. По-друге, метод легко «обдурити», якщо змінити вручну інформацію, яка потрапляє в заголовки відповідей. А це досить легко зробити для проектів з відкритим вихідним кодом. Крім того частина вразливостей може бути усунена розробниками, які при цьому не будуть змінювати версію, що потрапляє в заголовок.

Більш достовірним методом є активні зондувальні перевірки. Він полягає в порівнянні «цифрового зліпка» фрагмента ПЗ зі зліпком, який свідомо схильний до вразливості. Так працює більшість антивірусів. Вони порівнюють скановане ПЗ з сигнатурами відомих їм вірусів. Якщо сигнатури збігаються, значить, є ймовірність, що це вірус.

Прикладами швидших різновидів методу є перевірки контрольних сум або дат аналізованого ПЗ. Такі перевірки використовують сканери рівня ОС. Метод активних зондуючих перевірок менш швидкий, ніж перевірка заголовків і складніший в реалізації.

Метод під назвою «імітація атак» використовує інформацію про відомі атаки. Він задіюється, коли не можна однозначно сказати має сервіс вразливість чи ні без проведення пробної атаки. Цей метод найбільш точний, але виконується не так швидко як інші. Варто відзначити, що імітація атак не завжди здійсненна. Першою причиною є «відмова в обслуговуванні» перевіряємого компонента, а другий - «непридатність» вразливості для реалізації атаки.

Вибір методів для перевірки залежить від розглянутого компонента. Необхідно враховувати, що велика частина вразливостей не може бути встановлена без наслідків для функціонування сервісу. Якщо необхідно перевірити важливий, високонавантажений сервер, то проводити імітацію атак нерозумно, так як це може призвести до його виходу з ладу і точно ще більше його завантажить. Для аналізу такого сервера необхідно застосовувати менш «агресивні» перевірки, такі як активне зондування.

Система виявлення вторгнень (СВВ) або система виявлення атак (СВА) є програмним або апаратним засобом, що призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу. У разі апаратного рішення СВВ можуть вбудовуватися в систему обробки даних [3]. Програмні ж рішення працюють «по сусідству» з компонентами КПС.

СВВ використовується для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпечність комп'ютерної системи. До такої активності відносяться мережеві атаки проти

вразливих сервісів, атаки, спрямовані на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого ПЗ (комп'ютерних вірусів, троянів і черв'яків).

Зазвичай архітектура СВВ включає [4]: сенсорну підсистему, призначену для збору подій, пов'язаних з безпекою захищуваної системи; підсистему аналізу, призначену для виявлення атак і підозрілих дій на основі даних сенсорів; сховище, що забезпечує накопичення первинних подій і результатів аналізу; консоль управління, що дозволяє конфігурувати СВВ, спостерігати за станом захищуваної системи і СВВ, переглядати виявлені підсистемою аналізу інциденти.

За способами моніторингу IDS системи підрозділяються на мережеві системи виявлення вторгнень і системи виявлення вторгнень на рівні хоста [5]. Мережеві системи виявлення вторгнень аналізують мережевий трафік за даними сенсорів, розташованих у ключових вузлах мережі. Системи виявлення вторгнень на рівні хоста виявляють вторгнення за допомогою спеціальної служби, яка аналізує системні запити, логи активності додатків, зміни файлової системи і інші процеси, що відбуваються на рівні хоста.

Однак наявність додаткових мережевих пристроїв може бути недоліком для мереж малих підприємств.

При сигнатурному підході детектори атак аналізують діяльність системи, використовуючи для цього перевірку відповідності події або безлічі подій і заздалегідь визначеного зразка, який описує відому атаку. Відповідність зразка відомій атаці називається сигнатурою, визначення атаки або вторгнення називають "сигнатурним визначенням". Перевагами такого підходу є ефективне визначення атак і відсутність великого числа помилкових повідомлень, а також надійна діагностика використання конкретного інструментального засобу або технології атаки. Це дозволяє адміністраторам, незалежно від рівня їх кваліфікації, почати процедури обробки інциденту, а також скорегувати заходи забезпечення безпеки. Очевидним недоліком є обов'язкове оновлення бази даних для отримання нових сигнатур атак.

Метод аномалій полягає у визначенні ненормальної (незвичайної) поведінки на хості або в мережі. Детектори аномалій припускають, що атаки відрізняються від "нормальної" (законної) діяльності і можуть бути визначені системою, яка вміє відслідковувати ці відмінності. Вони використовують нормальну поведінку користувачів, хостів або мережних з'єднань і зберігають їх у так звані профілі. Профілі створюються за даними, зафіксованими в період функціонування КПС без втручання зловмисників. На етапі визначення аномалій детектори збирають дані про різні події в захищуваній системі і використовують різні метрики для оцінки величини відхилення. Перевага підходу полягає в здатності визначення атаки без знання конкретних деталей (сигнатури). До недоліків можна віднести можливість великої кількості помилкових сигналів у випадку спостереження непередбачуваної активності користувачів. Ще одним недоліком є додаткові часові витрати для навчання детектора [6].

Метод, заснований на політиках доступу, полягає в написанні правил мережевої безпеки в термінах розподілу доступу, наприклад, які мережі можуть взаємодіяти одна з одною і які протоколи при цьому можуть використовуватися. Перевагою є більш легке, ніж у методі аномалій, виявлення нових атак. Однак, як і в сигнатурному методі, великою складністю є створення і підтримка даних у базі політик.

У чистому вигляді СВВ є пасивним засобом захисту. Інциденти інформаційної безпеки фіксуються і передаються у вигляді звіту користувачеві ПК або адміністратора мережі. Логи про минулі події записуються в спеціальний розділ додатка і дублюються на панелі керування адміністратора. Сигнали про загрози безпеки даних не мають подальшої обробки в таких системах. Для безпосереднього захисту даних і боротьби з порушеннями інформаційної безпеки використовують активні засоби захисту, такі як системи запобігання вторгнень.

Системою запобігання вторгнень є програмний або апаратний засіб, який здійснює моніторинг мережі або комп'ютерної системи у реальному часі з метою виявлення, запобігання або блокування шкідливої активності. IPS веде відповідні дії на порушення. Це може бути скидання з'єднання або перенастроювання міжмережевого екрану для блокування вхідного трафіку від зловмисника. Протидія може починатися автоматично або по команді системного адміністратора [7].

Системи виявлення та системи запобігання вторгнень схожі як за класифікацією, так і за своїми функціями. Головна їх відмінність полягає в тому, що другі завжди працюють у режимі реального часу і здатні автоматично блокувати дії зловмисника.

Висновки

Проаналізовано вимоги до захищеності КПС і модель адаптивної безпеки, як ефективний підхід до забезпечення захисту КПС.

Розглянуті методи і засоби оцінки захищеності, що повинні функціонувати на всіх етапах атаки на КПС, мають грунтуватися на основних принципах забезпечення захисту і бути адаптивними до нових, невідомих погроз і атак.

На основі аналізу методів, використовуваних в системах ШІ, і їх застосовності для вирішення завдань контролю безпеки виділені методи на основі МАС, онтології і НС для подальшого використання в роботі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Васильківський М. В., Паламарчук Р. П. «Підвищення інформаційної безпеки у волоконно-оптичних системах передачі», Матеріали конференції «XLVIII Науково-технічна конференція підрозділів Вінницького національного технічного університету (2019)», Вінниця, 2019
2. Васильківський М.В., Паламарчук Р.П. Методи захисту волоконно-оптичних ліній зв'язку: тези XLVII Науково-технічної конференції факультету інфокомунікацій, радіоелектроніки та наносистем (м. Вінниця, 21.03.2018 – 23.03.2018) Вінниця, 2018.
3. Васильківський М. В., Паламарчук Р. П. Захист інформації у волоконно-оптичних системах зв'язку / Вісник Хмельницького національного університету. Технічні науки №3 2018р. с. 202-207.
4. Васильківський М. В., Паламарчук Р. П. Оцінювання енергетичних характеристик волоконнооптичних ліній зв'язку за критерієм коефіцієнта помилок / Вісник Хмельницького національного університету. Технічні науки №1 2019р. с. 216-220.
5. Васильківський М.В. Захист інформації у волоконно-оптичних лініях зв'язку/ М.В. Васильківський, Р.П. Паламарчук // Вимірювальна та обчислювальна техніка в технологічних процесах (ВОТТП_18_2018) XVIII міжнародної науково-технічної конференції, 8-13 червня 2018 р. – Матеріали – Одеса. – 2018 с. 209.
6. Петров С.А., Хорев П.Б. Побудова адаптівної захисту на базі багатоагентній системи // Праці 20 МНТК "Радіоелектроніка, електротехніка та енергетика", Видавничий дім МЕІ, 2014 року, Том 2, с. 35.
7. Petrov S.A. Building adaptive security system based on multi-agent system, materials of the second international research and practice conference. Vol. 2. Westwood - Canada, 2013. p. 196-201.

Васильківський Микола Володимирович - канд. тех. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, Вінниця, e-mail: mvasylkivskyi@gmail.com.

Стальченко Олександр Володимирович – канд. тех. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, Вінниця. e-mail: magicphenix@gmail.com.

Ремінський Олександр Васильович — студент групи ТКТ-19мс, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця. e-mail: sikuray77@gmail.com.

Vasylkivskyi Mikola V. – Phd, Assistant Professor of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia, e-mail: mvasylkivskyi@gmail.com.

Stalkhenko Alexander V. – Phd, Assistant Professor of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia, e-mail: magicphenix@gmail.com.

Reminsky Alexander V. – Department of Infocommunication, Electronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia, e-mail: sikuray77@gmail.com.