УДК 004.056

Юрій Петрович ГОРЕЛОВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-0330-5008

ДО ПИТАННЯ РОЗРОБКИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ КІБЕРЗАХИСТУ

У зв'язку з безпрецедентно швидким розвитком комп'ютерних і телекомунікаційних технологій, у тому числі мережі Інтернет, що поєднує величезну кількість різнорідних мереж (від локальних до транснаціональних), і переходом до інформаційного суспільства проблема забезпечення кібербезпеки та побудови інформаційно-безпечних розподілених обчислювальних систем стала однією з найбільш актуальних проблем.

Відповідно до сучасних поглядів перспективна система кіберзахисту повинна бути взаємопов'язаною, багаторівневою та безупинно контрольованою системою, здатною оперативно реагувати на віддалені й локальні кібератаки та несанкціоновані дії, накопичувати знання про способи протидії, виявлення та реагування на атаки й несанкціоновані дії та використовувати їх для посилення захисту.

Така система повинна надавати, принаймні, три рівні захисту. Перший рівень захисту становлять «традиційні» засоби захисту, що реалізують функції ідентифікації й аутентифікації, криптографічного захисту, розмежування доступу, контролю цілісності, реєстрації й обліку, міжмережевого екранування. Другий рівень включає засоби проактивного захисту, що забезпечують збір необхідної інформації, аналіз захищеності, моніторинг стану мережі, виявлення атак, протидію їхньої реалізації, введення зловмисника в оману й т.п. Третій рівень відповідає засобам керування захистом, які здійснюють інтегральну оцінку стану мережі, керування захистом й адаптацію політик безпеки й компонентів системи кіберзахисту.

Перший рівень досить широко представлений в теперішній час. Розробка механізмів кіберзахисту, що ставляться до другого й особливо третього рівню, що реалізують власне кажучи інтелектуальну надбудову над традиційними механізмами захисту (для керування ними), становить у цей час пріоритетне завдання в області теоретичних і прикладних досліджень з побудови інформаційно-безпечних розподілених обчислювальних систем.

У цей час для рішення цих завдань усе активніше використаються підходи, засновані на методах, засобах та алгоритмах, розроблених у рамках штучного інтелекту: нейронні мережі, бази знань, інтелектуальні агенти, системи продукційних правил й ін.

Ці підходи активно використовуються не тільки для створення засобів захисту другого й третього рівня, але й для вдосконалювання засобів захисту першого рівня [1-3]. Тут широко використовуються алгоритми машинного навчання, прийняття рішень й аналізу даних.

Система, що реалізує інтелектуальні механізми захисту повинна реалізовувати наступні функції:

1) збір інформації про стан інформаційної системи і її аналіз за рахунок механізмів обробки й об'єднання інформації з різних джерел;

2) проактивне попередження атак і перешкоджання їхньому виконанню;

3) виявлення аномальної активності і явних атак, а також нелегітимних дій і відхилень роботи користувачів від політики безпеки, пророкування намірів і можливих дій порушників;

4) активне реагування на спроби реалізації дій порушників шляхом автоматичної реконфігурації компонентів захисту для відбиття дій порушників у реальному масштабі часу;

5) дезінформацію зловмисника, приховання й камуфляж важливих ресурсів і процесів, «заманювання» зловмисника на помилкові компоненти з метою розкриття й уточнення його цілей, рефлексивне керування поведінкою зловмисника;

6) моніторинг функціонування мережі та контроль коректності поточної політики безпеки й конфігурації мережі;

7) підтримка прийняття рішень з керування політиками безпеки, у тому числі з адаптації до наступних вторгнень і посилення критичних механізмів захисту.

Перспективним підходом до побудови інтелектуальних механізмів кіберзахисту є технологія інтелектуальних багатоагентних систем. Цей підхід дозволяє в порівнянні із традиційними методами істотно підвищити ефективність захисту інформації, у тому числі її адекватність, відмовостійкість, стійкість до деструктивних дій, універсальність, гнучкість і т.д.

Відповідно до даного підходу передбачається, що компоненти систем кіберзахисту, спеціалізовані по типах розв'язуваних завдань, тісно взаємодіють один з одним з метою обміну інформацією й прийняття погоджених рішень, адаптуються до зміни трафіку, реконфігурації апаратного та програмного забезпечення, новим видам кібератак. Компоненти багатоагентної системи кіберзахисту являють собою інтелектуальні автономні програми (агенти захисту), що реалізують певні функції захисту з метою забезпечення необхідного класу захищеності. Вони дозволяють реалізувати комплексну надбудову над механізмами безпеки мережних програмних засобів, операційних систем і додатків, підвищуючи захищеність системи до необхідного рівня.

У прийнятій архітектурі в явному виді відсутній «центр керування» колективом агентів – залежно від сформованої ситуації ініціативу обробки може брати на себе кожен з агентів, що ініціює й

(або) реалізує функції кооперації і керування. Якщо буде потреба, агенти можуть як клонуватися (утворювати нові сутності), так і припиняти своє функціонування. Залежно від ситуації (виду й кількості атак на комп'ютерні мережі, наявності обчислювальних ресурсів для виконання функцій захисту) може знадобитися генерація декількох екземплярів агентів кожного класу.

Такий підхід дозволяє створити систему з розширюваною адаптивною архітектурою для виявлення атак різних видів.

Список бібліографічних посилань

1. Csubak D., Szucs K., Voros P. and Kiss A. Big Data Testbed for Network Attack Detection. *Acta Polytechnica Hungarica*. 2016. № 13. P. 47-57.

2. Chen Z., Xu G., Mahalingam V., Ge L., Nguyen J., Yu W. and Lu C. A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures. *Big Data Research*. 2016. № 3. P. 10-23.

3. Singh K., Guntuku S.C., Thakur A. and Hota C. Big Data Analytics Framework for Peer-to-Peer Botnet Detection using Random Forests. *Information Sciences*. 2014. № 278. P. 488-497.

Одержано 30.10.2018

УДК 004.056.53

Захар Георгійович ДЕМИДОВ,
науковий співробітник науково-дослідної лабораторії захисту інформації та кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
Олексій Володимирович ХЛЕСТКОВ,
старший науковий співробітник науково-дослідної лабораторії захисту інформації та кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

АКТУАЛЬНІСТЬ XSS-АТАК ТА СПОСОБИ ЗАХИСТУ ВІД НИХ

Web-додатки є одними з найбільш небезпечних систем на сьогоднішній день. І, звичайно, хакери цим користуються. Одним з видів атак на додаток є міжсайтовий скриптинг або XSS атака. Зараз вони складають близько 15% всіх атак виявлених вразливостей сайтів.

XSS атака – це атака на вразливість, яка існує на сервері, що дозволяє впровадити в генеруєму сервером HTML-сторінку якийсь довільний код, в якому може бути взагалі все що завгодно і передавати цей код в якості значення змінної, фільтрація по якій не працює, тобто сервер не перевіряє дану змінну на наявність в ній заборонених знаків -, <,>, ', ".

Значення цієї змінної передається від генеруємої HTML-сторінки на сервер в скрипт, її викликавший шляхом відправки запиту. А далі починається найцікавіше для зловмисника. PHP-скрипт у відповідь на даний запит генерує HTML-сторінку, в якій відображаються значення