УДК 004.77

Станіславчук Д. О., здобувач вищої освіти;
Крижановський В Г., д-р техн. наук, професор,
професор кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ПОБУДОВА «АГЕНТІВ» ДЛЯ SIEM З МЕТОЮ РОЗШИРЕННЯ ГАЛУЗІ ЇХ ВИКОРИСТАННЯ

Ключові слова: SIEM, агенти, атаки.

Вступ. З ростом загроз кібербезпеці та необхідністю захисту інформаційних ресурсів стає все актуальнішою роль SIEM-систем. Важливими інструментами для збору інформації про інформаційну систему є SIEM-агенти. Ця доповідь розглядає особливості, пов'язані із захистом агентів та інформації, яку вони обробляють, зокрема це важливо під час ефективної та безпечної обробки даних.

Актуальність. Сьогодні інформація є найважливішим ресурсом людства. В сучасному світі, де кількість інформації постійно зростає, захист і забезпечення безпеки інформації стає дедалі більш важливим завданням. З огляду на те, що кількість нових видів атак постійно зростає, використання та забезпечення агентів SIEM стає необхідністю для підприємств і організацій будь-якого розміру.

Мета – визначення завдань для коректної та безпечної роботи агентів, розгляд можливостей збільшення функціоналу агентів.

SIEM-агенти – програмне забезпечення, яке збирає логи (журнали подій) та передає їх інструментам SIEM для аналізу. Їх основною особливістю є нормалізація – фільтрація та представлення логів у вигляді, який полегшить роботу інших SIEM-інструментів [1].

Агентів класифікують відповідно до способу, яким вони передають логи для колекторів (Log collector – інструмент SIEM, який аналізує логи, отримані від агентів). Їх поділяють на 2 типи: «pull» та «push». «Pull» – спосіб, за якого колектор самостійно звертається до агента для отримання логу. Цей спосіб надає більшу гнучкість у налаштуванні отримання логів. Наприклад, колектор не звертатиметься, коли використовується занадто багато ресурсів системи. Наступний спосіб – «push» – агенти самостійно відправляють логи до колектора, не очікуючи запиту. Цей спосіб є швидшим, оскільки не вимагає формування запиту [2].

Оскільки агенти оперують інформацією про стан інформаційної системи, їх потрібно вважати окремими елементами цієї системи. Звідси виникають завдання із забезпечення їх захищеності, швидкодії та надійності.

Забезпечення захищеності. Забезпечення захищеності, як будь-якого інформаційного ресурсу, означає забезпечення конфіденційності, цілісності та доступності інформації. Якщо виділяти специфічні завдання для агентів, необхідно: забезпечити секретність під час збору та передачі логів, забезпечити від несанкціонованого видалення та санкціонованості джерела.

Для забезпечення захищеної передачі лініями зв'язку можна використовувати мережеві протоколи захисту або інші методи шифрування. До того ж потрібно забезпечити секретність даних ще до передачі – на самому пристрої. Вирішення цієї проблеми запропонували Шнайер та Келсі [3]. Для шифрування логу цей алгоритм використовує симетричний алгоритм шифрування (наприклад, DES), а для цифрового підпису асиметричний алгоритм (наприклад, RSA). Суть роботи алгоритму: агент формує ключ A_0 та передає його колектору, на основі цього формуються ключі шифрування за принципом $A_i = hash(A_{i-1})$, де $hash$ – функція хешування. Після отримання A_i A_{i-1} знищується. Автори пояснюють, що навіть якщо агент буде скомпрометований, зловмисник не зможе визначити попередні ключі, а отже, й не зможе розшифрувати попередні логи. Важливо зазначити, що якщо цей алгоритм використовує цифровий підпис, за допомогою нього ми можемо встановити відправника повідомлення, а також визначити, чи всі логи були доставлені.

Забезпечення швидкодії. Питання швидкодії завжди було важливим для агентів. Оскільки вони є окремими застосунками, то будуть навантажувати систему; питання лише в тому, чи є це прийнятним.

Під час оцінки швидкодії ключовим показником є EPS (Event per second) – кількість подій за секунду, яку може виконати система або застосунок. Якщо йдеться про агентів – скільки логів за секунду він може обробити. Якщо, наприклад, у звичайних роутерах кількість подій у секунду зазвичай доволі низька (в середньому 0,6, пікове навантаження – 380,5), то фаєрволи можуть бути розраховані на сотні тисяч одночасних підключень [4]. Для покращення швидкодії можна розглядати 2 варіанти: збільшення ресурсів пристрою або фільтрацію логів. Із першим варіантом зрозуміло – збільшення ресурсів означає збільшення можливостей обрахунків, що збільшує кількість обробки можливих подій. Другий варіант – введення правил щодо збору та обробки логів. В основі цього способу лежить можливість агентів обирати: які логи будуть відправлятись, який пріоритет у відправки, які логи будуть шифруватись та ін. Цей спосіб не збільшить EPS, але він дасть нам змогу правильно розподілити ресурси, якими ми володіємо, що загалом може збільшити швидкодію.

Забезпечення надійності. Надійність агентів – здатність зберігати параметри в часі, що дає їм змогу правильно виконувати покладені на них функції [5]. Покращення надійності можна поділити на два рівні: програмний рівень та рівень політик. Програмний рівень – це надійність на рівні коду, тобто помилки, вразливості, оптимізація. Усе це покладається на компанію яка поставляє послуги SIEM: вони повинні покращувати свої програмні продукти. Рівень політик стосується політик безпеки компанії, яка використовує агентів. На цьому рівні компанія повинна забезпечувати виконання вимог технічної документації на продукт, проводити оновлення програмного забезпечення, забезпечувати ресурсами необхідними для роботи. Дотримання вимог на обох рівнях повинно дати змогу забезпечити надійність системи.

Варіанти реалізації агентів завдяки розширенню їх функціоналу. Зараз агенти мають доволі невеликий функціонал – це пов'язано з чіткою структурою

SIEM, а також тим, що частина інструментів виноситься для обробки в хмарі, що є зручним рішенням для багатьох компаній.

Агенти з функціями безпеки. Інструменти SIEM зазвичай розташовуються на окремих серверах, що пов'язано з тим, що вони обробляють велику кількість інформації. Але якщо організація має малу кількість елементів мережі, що робить встановлення сервера для SIEM дороговартісним, альтернативою може бути наділення агентів функціями безпеки. Для цього потрібно реалізувати дві функції: аналіз логів та реагування на інциденти. По суті, реалізується мініатюрна SIEM-система на кожному пристрої.

Агенти з обмеженими функціями безпеки. Ці агенти не будуть виконувати всіх функцій SIEM, але можуть збільшити швидкодію SIEM-системи. Суть їх у тому, щоб вони могли автоматично аналізувати та реагувати на деякі кібератаки. Наприклад, агент реєструє аномальну велику кількість входів одночасно на деякий сервер. Імовірно, відбувається DDoS-атака, і замість того, щоб надсилати логи до колектора, що займає час, агент може автоматично надіслати звіт про те, що на пристрій відбувається атака, або самостійно ввести якісь дії. Цей спосіб може пришвидшити процес реагування на інциденти.

Висновки

SIEM-агенти в системах безпеки відіграють важливу роль, забезпечуючи збір та передачу логів для подальшого аналізу. Для їх успішної роботи важливі аспекти захищеності, швидкодії та надійності. Розширення функціоналу агентів може значно змінити можливості агентів, що дає змогу використовувати їх зовсім по-іншому. Це може покращити деякі показники системи.

Список використаних джерел

1. Dorigo S. Radboud University Nijmegen Security Information and Event Management Master Thesis. 2012.

2. Karlzén H. An Analysis of Security Information and Event Management Systems – The Use or SIEMs for Log Collection, Management and Analysis. 2009.

3. Schneier B., Kelsey J. Cryptographic Support for Secure Logs on Untrusted Machines. USENIX Security Symposium. 1998.

4. Butler M. J. Benchmarking Security Information Event Management (SIEM). 2009.

5. Zahedi F. Reliability of Information Systems Based on the Critical Success Factors – Formulation. MIS Quarterly, 1987. № 11(2). P. 187–203. DOI: 10.2307/249362.