Проблеми впровадження системи аналітики поведінки користувачів та сутностей

Ігор Пасєка[1], Олександр Сєвєрінов[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м Харків, пр. Науки, 14, E-mail: ihor.pasieka@nure.ua

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м Харків, пр. Науки, 14, E-mail: oleksandr.sievierinov@nure.ua

Коротка анотація – Issues of implementation of behavior and object analysis systems (UEBA) are considered. The main tasks and components of UEBA systems are considered. The problems that arise when implementing these systems in the organization are analyzed.

Ключові слова - аналітика поведінки користувачів, аналітика поведінки сутностей, UBA, UEBA, внутрішній порушник, інсайдер.

I. Вступ

Останнім часом все більше посилюється небезпека втручання в роботу інформаційних систем в формі несанкціонованого доступу до інформації, в результаті чого кількість витоків конфіденційної інформації з кожним роком зростає. Так за результатами глобального дослідження, проведеного аналітичним центром InfoWatch, у першому півріччі 2019 року зареєстровано 695 витоків інформації, причиною яких став внутрішній порушник (55,6% від загального числа зареєстрованих випадків) та 555 випадків (44,4%) витоку інформації, що стався через зовнішній вплив (рис. 1) [1].

Засоби антивірусного захисту, міжмережні екрани, системи виявлення вторгнень призначені для протидії вірусам і хакерам. Однак вони не захищають від крадіжки інформації власними співробітниками (інсайдерами).

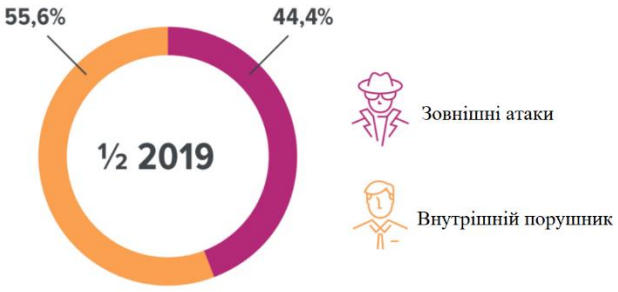

Рисунок 1 – Види порушників при витоку інформації

Одним з найбільш ефективних методів боротьби з несанкціонованим витоком інформації з урахуванням необхідності контролю своїх співробітників є впровадження систем аналітики поведінки користувачів та сутностей – User and Entity Behavior Analytics (UEBA)) [2, 3].

Тому актуальним є проведення аналізу систем UEBA та проблемних питань аналітики поведінки користувачів та сутностей.

II. UEBA - системи аналітики поведінки користувачів та сутностей

Існуючи до недавнього часу на ринку системи інформаційної безпеки, такі як DLP та IAM системи, SIEM рішення, антивірусні та IDS/IPS засоби не можуть у повній мірі вирішити проблеми протидії внутрішнім порушникам. Тому з 2014 року на ринку стали з'являтися системи аналітики поведінки користувачів та сутностей – UEBA. Спочатку вони з'явилися у вигляді модулів для DLP і SIEM систем, мали назву UBA (User Behavior Analytics) та здійснювали тільки аналіз поведінки користувачів. Інші виробники подібних систем називали свої рішення з поведінкового аналізу SUBA (Security User Behavior Analytics) (Forrester), Advanced Analytics або Advanced Threat Analytics (Exabeam і Microsoft) [4].

На даний час системи UEBA являються як окремими рішеннями, так і функціями, що вбудовані в інші платформи безпеки.

Використання UEBA-систем дозволяє перейти до пошуку аномалій не тільки в поведінці користувачів, але і сутностей, до яких відносять робочі станції, мережне обладнання, програмне забезпечення, мережний трафік та інше. Ці рішення дозволяють захиститися від самих різних загроз, таких як несанкціонований доступ та виток конфіденційної інформації, шахрайські дії, крадіжки прав доступу, дії вірусів та шкідливого ПЗ і багато інших.

Враховуючи величезну кількістю даних, що постійно генеруються в інформаційній системі, обробляти їх в ручному режимі неможливо. Тому UEBA-системи набирають популярність.

На даний час системи UEBA вирішують основні завдання [5]:

- аналітика даних з різних джерел (статистична або з використанням методів машинного навчання) в реального часу і/або періодично;
- ідентифікація атак і інших порушень та витоків інформації;
- оперативна пріоритизація подій, отриманих з різних джерел, та видача їх адміністратору інформаційної безпеки;
- надання адміністраторам інформаційної безпеки розширеної інформації про інциденти, яка включає всі об'єкти, що були залучені в аномальну активність.

Дослідницька компанія Gartner розглядає системи UEBA як поєднання трьох компонентів, які включають задачі, що вирішуються, аналітику і джерела даних (рис. 2).

Виходячи з проведених досліджень компанією Gartner, UEBA рішення можуть вирішувати широкий спектр завдань [5]. Але основне застосування даних систем включає виявлення різних категорій загроз при аналізі поведінки користувачів і сутностей:

- неавторизований доступ і переміщення даних;
- підозрілу поведінку привілейованих користувачів;
- шкідливі або неавторизовані дії співробітників;
- нестандартний доступ і використання хмарних ресурсів.

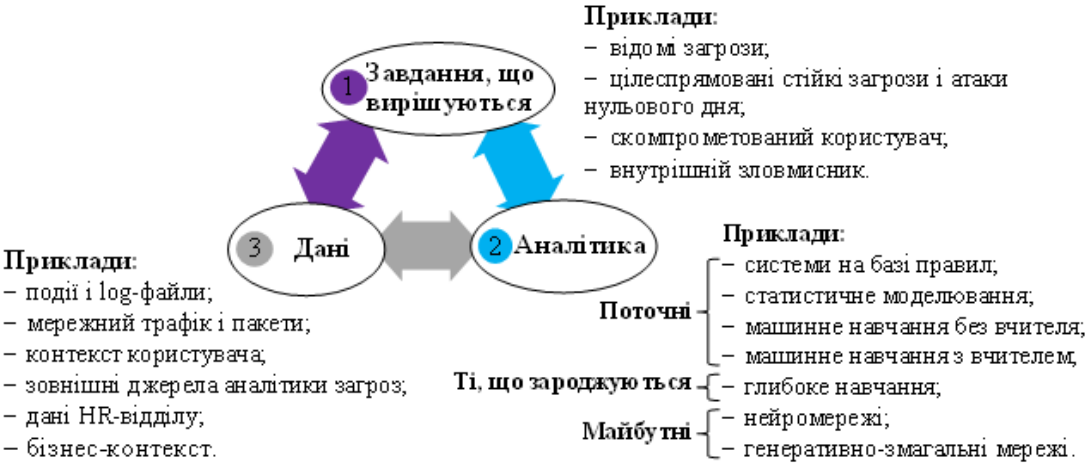

Рисунок 2 – Компоненти системи UEBA

III. Проблеми впровадження UEBA рішень

Проведений аналіз показав, що одними з основних проблем широкого застосування UEBA рішень є їх висока вартість, складне впровадження, обслуговування і використання. Розмір вкладень часу і ресурсів в інструменти UEBA залежить від поставлених завдань і типів аналітики, які необхідні для їх вирішення, і найчастіше вимагають великих витрат. Також, як показує аналіз відгуків користувачів даних систем, час впровадження і повсякденне використання UEBA рішень може бути більш трудомістким і віднімати більше часу, ніж обіцяє виробник, навіть якщо розглядати тільки базові моделі виявлення загроз [5]. Так потрібно від 3 до 6 місяців для запуску UEBA системи з нуля до отримання перших результатів вирішення стандартних завдань. Для більш складних завдань, таких як виявлення інсайдерських погроз в організації, термін може збільшуватися до 18 місяців.

При цьому на ще більше ускладнюють можливість впровадження і ефективність використання систем UEBA такі фактори:

- складність архітектури організації, інформаційної системи та протоколів управління даними;
- доступність даних, потрібних для аналітики UEBA;
- складність алгоритмів аналітики UEBA від виробника та кількість попередньо настроєної аналітики;
- наскільки просто інтегрувати UEBA рішення в вже наявні в організації системи безпеки й аналітики.

На основі проведених досліджень компанія Gartner, враховуючи перелічені проблеми, робить прогноз майбутнього застосування систем аналітики поведінки користувачів та сутностей [5]:

- до 2020 року до 95% всіх впроваджених UEBA-рішень буде складовою частиною інших платформ безпеки (CASB, DLP, EDR, NTA, SIEM);
- до 2021 року ринок систем UEBA як самостійних продуктів, припинить своє існування і буде існувати тільки як інші рішення безпеки з функціоналом UEBA.

Висновки

Таким чином, незважаючи на існуючу потребу в інструментах системи аналітики поведінки користувачів та сутностей та враховуючи існуючі проблеми впровадження UEBA рішень, найбільш імовірно використання в майбутньому функціонала UEBA тільки як складовою частини інших платформ безпеки.

Література

[1] Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. Сайт компанії InfoWatch [Електронний ресурс]. – Режим доступу: https://infowatch.com.

[2] Johansen G. Digital forensics and incident response: an intelligent way to respond to attacks. – 2017.

[3] Сєвєрінов О.В. Аналіз систем аналітики поведінки користувачів і сутностей / О.В. Севєрінов, І.В. Пасєка // Інформатика, управління та штучний інтелект. Тези шостої міжнародної науково-технічної конференції – Х.: НТУ «ХПІ», 2019. – С. 108.

[4] Обзор рынка систем поведенческого анализа — User and Entity Behavioral Analytics (UBA/UEBA) [Електронний ресурс]. – Режим доступу: https://www.antimalware.ru/analytics/Market_Analysis/user-andentity-behavioral-analytics-ubaueba

[5] Сайт компанії Gartner [Електронний ресурс]. – Режим доступу: https://www.gartner.com/.