УДК 004.056

UBA-АНАЛІЗ ЯК ЗАСІБ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ

Грицаненко Я.Ю.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
каф. КРіСТЗІ, м. Харків, Україна
тел. +38(057) 702-14-30, e-mail: yaroslav.hrytsanenko@nure.ua

The principles of UBA-analytics operation are considered, as well as tasks that UBA-systems should solve to ensure information security in automated of military automated systems.

Кілька років тому на зарубіжному і зовсім нещодавно на вітчизняному ринку інформаційних систем забезпечення безпеки з'явився новий клас рішень. Основний наголос ці рішення роблять на аналіз поведінки– UBA – User Behavior Analytics.

Перше, що має робити UBA, – це, накопичуючи в процесі роботи або використовуючи раніше накопичені дані, за допомогою закладених методів визначати характерну стабільну поведінку об'єктів. І не важливо, чи це користувачі це, програмні чи апаратні засоби.

Для аналізу UBA системі потрібні джерела різноманітних даних за значний часовий період, щоб на їх підставі можна було визначити звичайну для користувача або сутності поведінку та її межі, вихід за які вважатиметься відхиленням від норми. Залежно від методів аналізу, що використовуються, підходи в рішеннях UBA можуть різнитися.

Вважається, що чим більше джерел постачають дані в UBA, тим краще. Це неоднозначний висновок, оскільки підключення великої кількості джерел призводить до збільшення часових затрат на інтеграцію та інтерпретацію розрізненої інформації для єдиної мети поведінкового аналізу. Тут слід говорити про достатність даних для обробки. Адже надмірність інформації не тільки збільшує обсяги та тривалість обчислень, а й може спричинити таке нагромадження результатів, з якими у співробітника безпеки просто не буде часу та можливості розібратися.

Допускається, що рішення UBA можуть видавати результати аналізу з певною періодичністю, але чим оперативніше вони це роблять, тим вигідніше виглядають.

Друге, що очікується від рішень UBA – це здатність детектувати нетипову або, іншими словами, аномальну поведінку. У відкритих джерелах часто висловлюється думка, що за результатами детектування UBA можуть ховатися серйозні порушення, які погано виявляються традиційними засобами безпеки.

Третє, що можуть надати рішення UBA – приоритизація отриманих результатів. Багато систем безпеки дуже чуйно реагують на всілякі зміни,

що призводить до генерації великої кількості попереджень. Таких попереджень буває настільки багато, що співробітники безпеки просто не мають часу на їх розбір і ретельне розслідування. Рішення UBA здатні консолідувати попередження, оцінювати їх ризики, розставляти пріоритети та звертати увагу користувача лише на найсерйозніші відхилення. Внаслідок цього зростає ефективність роботи служб безпеки за рахунок зниження кількості помилкових спрацьовувань.

І, звичайно, будь-яке технологічне рішення має видавати кінцевий результат. У випадку UBA – надавати фахівцю з безпеки весь контекст виявлених аномалій. Контекст буде змінюватись в залежності від можливостей конкретного рішення та конкретної інсталяції.

Мінімальний очікуваний результат від використання рішень UBA зводиться до того, щоб UBA-рішення надавали для розслідування інформацію про всіх користувачів та сутностей, пов'язаних з детектованим поведінковим відхиленням. Відомості про дії персоналій та результати цих дій значно збагачують контекст. Розвинені рішення UBA повинні інформувати фахівців безпеки про все «оточення» виявленої аномалії, що включає всі, що лежать поруч у часі і пов'язані за певними ознаками групи та ланцюжка поведінкових відхилень.

Також враховується і те, що рішення UBA не повинні бути вузькими у застосуванні та повинні мати декілька напрямків використання.

Фахівці в галузі інформаційної безпеки виділяють такі функції, наявність яких у сучасних UBA рішеннях вітається:

1) використання вбудованих моделей поведінки; 2) оповіщення / повідомлення користувача про виявлення поведінкових відхилень; 3) наявність гнучкого пошуку щодо розслідувань; 4) формування звітності за наслідками аналізу; 5) використання часової шкали (timeline) для аналізу одержаних результатів у часі; 6) ретроспективний аналіз раніше накопичених даних виявлення поведінкових відхилень у минулому.

Гнучкість рішень UBA, що виражається в адаптивності до поступовій зміні об'єктів аналізу та наявності можливості розширення та уточнення моделей поведінки, є додатковою перевагою.

У перспективі від UBA-рішень очікується підтримка хмарних сервісів. Йдеться про наявність функціоналу CASB – систем забезпечення безпечного доступу до хмар, що виділяються в окремий клас рішень.

Також просувається концепція використання UBA-рішень для Інтернету речей (IoT).

У рамках розуміння застосування рішень UBA, що склалося, виділяють наступні напрямки використання цієї нової технології:

1. Збір та надання інформації про поведінку. Дослідження особливостей поведінки як користувачів, так і інших сутностей саме собою представляє інтерес для фахівців з безпеки. Зазвичай характер поведінки відповідає виконуваним бізнес-функцій сутності. Різка розбіжність