ДОСЛІДЖЕННЯ СИСТЕМ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ

Савченко О.В.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, навчально-наукова лабораторія «Систем технічного захисту інформації (відеоспостереження, охоронні сигналізації і контроль доступу)», тел. (057) 702-14-78

The work considers the class of information security systems based on the analysis of data on the behavior of users and IT entities.

В наш час сформувався самостійний клас систем інформаційної безпеки, в основі яких лежать методи машинного навчання для виявлення ознак невластивої поведінки користувачів. Компанія Gartner даний клас систем позначає як UBA (User Behavior Analytics – аналіз поведінки користувачів). Використання UBA-систем дозволяє відійти від традиційного підходу з пошуку конкретних загроз і перейти до пошуку аномалій у поведінці користувачів. Популярність і ефективність даного підходу забезпечені насамперед величезною кількістю даних (у тому числі різних логів від систем захисту інформації), які характеризують користувача, але які вже неможливо обробляти в ручному режимі.

На підготовчій стадії, використовуючи алгоритми машинного навчання, UBA сервіс визначає типову поведінку для кожного суб'єкта і асоційованих додатків. Розраховуються базові критерії типової поведінки, відхилення від якої можна виміряти. Далі в рамках кожної користувальницької сесії проводиться постійний аналіз дії кожного суб'єкта, виконується порівняння наявних моделей профілю користувача з характеристиками виконуваних операцій з метою виявлення аномальної, підозрілої або потенційно ризикованої поведінки. Виявивши відхилення, сервіс поведінкового аналізу запускає інтелектуальну реакцію.

Таким чином, UBA-системи призначені для детального аналізу всіх дій, пов'язаних з конкретними користувачами, включаючи аналіз використання конкретних файлів і даних, використовуваних ними пристроїв, моніторинг процесів і запущених додатків, аналіз мережевого трафіку і т.д. На виході аналітик інформаційної безпеки, обслуговуючий UBA-системи, буде мати попередження про аномальному поведінку конкретних користувачів, з оцінкою ризику такої поведінки і докладними даними, пояснюючими що в поведінці користувача є аномалією, коли це почалося і як часто повторювалося. Всі ці дані дозволять ще на ранньому етапі припинити багато спроб порушення інформаційної безпеки, а також провести якісні розслідування інцидентів, що вже трапилися.

З часом на ринку з'явився модернізований клас UBA-систем, званий UEBA-системами (User Entity and Behavior Analytics) – поведінкова

аналітика користувачів та IT-сутностей. Причиною появи UEBA-систем став той факт, що розробники і фахівці з інформаційної безпеки усвідомили, що аналізу тільки поведінки користувачів недостатньо для виявлення всіх можливих атак і самих хитрих інсайдерів. Принцип дії цього класу систем дуже схожий на UBA-системи – це глибокий поведінковий аналіз, в якому нарівні з поведінкою користувачів аналізується дані про активність різних IT-сутностей, таких як АРМ кінцевих користувачів, сервери, бізнес-додатки, бази даних, облікові записи та інші. Джерела вхідних даних для UEBA-систем в цілому аналогічні UBA-систем.

Для проведення ефективного аналізу UEBA-системи вимагають великої кількості даних, зібраних з різних джерел. Чим більше інформації про користувачів передається в систему аналізу і чим більше додатків виявляються в поле її зору, тим вище стає ефективність і швидкість виявлення фактів підозрілої поведінки. Задачу збору та систематизації таких даних вирішують системи класу Security Information and Event Management (SIEM), надають доступний в базових конфігураціях інструментарій зі збору та штатного аналізу великих даних. Тому найбільш ефективним механізмом впровадження UEBA є їх тісна інтеграція з уже існуючими SIEM-системами, які в свою чергу використовують велику кількість джерел даних, забезпечуючи максимально повне охоплення подій, що реєструються в IT-інфраструктурі. Крім того, виробники UEBA-систем, що фокусуються на внутрішні загрози, як джерела інформації часто використовують не тільки системні журнали, а й зміст листування з корпоративної пошти і месенджерів, що дозволяє будувати більш детальні і персоніфіковані моделі поведінки користувачів.

Таким чином, UBA і UEBA-системи дуже схожі між собою, але все ж кардинально різняться в одному аспекті: UBA-системи акцентуються на користувачів і аномалії в їх поведінці, а всі дані про IT-інфраструктуру є лише доповненням для виявлення поведінкових аномалій користувачів. UEBA-системи IT-сутності розглядають нарівні з користувачами і відповідно будують моделі їх нормальної поведінки, що дозволяє UEBA-систем виявляти найвитонченіші і непомітні загрози інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Shashanka M., Shen M., Wang J. User and entity behavior analytics for enterprise security // 2016 IEEE International Conference on Big Data (Big Data), Washington, DC. 2016. P. 1867-1874.

2. Gartner. UEBA tool architecture. Режим доступу: https://www.gartner.com/

3. Cyber Security Insider “2018 insider threat report” // Режим доступу: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf