Перспективы применения и сценарии использования анализа поведения пользователей в сфере информационной безопасности

Д.А. Барабанов
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: dbarabanov7@gmail.com

Т.А. Иванова
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: Iv_tatyana@list.ru

Р.А. Гараев
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: garaevra@mail.ru

Аннотация[1]

В статье рассматривается класс систем информационной безопасности, основанных на анализе данных о поведении пользователей и ИТ-сущностей. Анализируется принцип работы таких систем и сценарии возможного использования. Особое внимание уделяется перспективам применения систем анализа поведения пользователей при обеспечении информационной безопасности крупных предприятий.

Ключевые слова: UBA; UEBA; машинное обучение; data science; внутренний нарушитель; инсайдер.

1. Введение

Суммы, которые тратят компании на информационную безопасность, значительно растут с каждым годом, при этом исторически акцент прежде всего делался на защите периметра организации от внешних угроз, но в последнее время тенденция меняется. Классические методы, основанные на правилах, сигнатурах и человеческом анализе данных постепенно уходят в прошлое, а основанные на них системы защиты информации, такие как системы обнаружения/предупреждения вторжений, межсетевые экраны и SIEM-системы, уже не обеспечивают достаточный уровень защиты от достаточно изощренных внешних и внутренних злоумышленников.

По данным отчета “2018 insider threat report” компании Cyber Security Insider 90% опрошенных компаний осознают уязвимость перед внутренними нарушителями, а 53% опрошенных подтвердили атаки, совершенные внутренними злоумышленниками, при этом стоит отметить, что ущерб от этих атак зачастую серьезно превышал ущерб, нанесенный внешними злоумышленниками. По данным того же отчета 86% опрошенных компаний либо уже имеют, либо внедряют системы защиты от внутренних угроз. При этом компании больше опасаются не злонамеренных инсайдеров, а халатных работников и подрядчиков, которые непреднамеренно становятся причиной взломов и утечек, несущих огромные убытки и в финансовом и в репутационном плане. Таким образом, можно сделать вывод, что компании приходят к пониманию риска, исходящего именно от легальных пользователей, и к осознанию того, что имеющиеся меры защиты против них неэффективны.

2. Анализ поведения, как средство борьбы с внутренними нарушителями

В той или иной степени, проблему внутренних нарушителей могут решать DLP-системы, IAM-

Труды Седьмой всероссийской научной конференции "Информационные технологии интеллектуальной поддержки принятия решений", 28-30 мая, Уфа-Ставрополь, Ханты-Мансийск, Россия, 2019

системы, SIEM-платформы, IDS/IPS-системы и прочие, однако с 2016 года на рынке стали появляться модули для DLP-систем и SIEM-платформ, и даже полностью самостоятельные системы, называемые UBA (User Behavior Analytics), основанные на анализе поведения пользователей. Важную роль в появлении этого класса систем сыграло развитие методов ИИ и data science. Таким образом, использование UBA -систем позволяет отойти от традиционного подхода по поиску конкретных угроз и перейти к поиску аномалий в поведении пользователей. Популярность и эффективность данного подхода обеспечены прежде всего огромным количеством постоянно генерируемых данных (в том числе различных логов от систем защиты информации), которые характеризуют пользователя, но которые уже невозможно обрабатывать в ручном режиме.

Суть методов анализа поведения в общем сводится к сбору огромного количества информации от всевозможных источников и на основе методов машинного обучения построению модели нормального поведения каждого. Источниками входных данных могут выступать Active Directory, DNS и DHCP-сервера, межсетевые экраны, прокси-сервера, системные журналы с АРМ пользователей и серверов, а также данные DLP и SIEM систем. Период построения первоначальных моделей нормального поведения занимает достаточно длительное время (от нескольких недель до нескольких месяцев), но при этом UBA-система будет учитывать контекст и специфику конкретной организации, в которую будет внедряться система.

После построения первоначальной модели нормального поведения, происходит постоянное сравнение данных текущего поведения пользователя с имеющейся моделью с целью выявления аномалий в поведении, а также дополнение и дообучение имеющейся модели новыми данными. В результате в каждый момент времени каждый пользователь будет иметь определенную оценку, характеризующую уровень риска, которая будет возрастать при наличии аномального поведения и снижаться при поведении стабильном.

Таким образом, UBA-системы предназначены для детального анализа всех действий, связанных с конкретными пользователями, включая анализ использования конкретных файлов и данных, используемых ими устройств, мониторинг происходящих процессов и запущенных приложений, анализ сетевого трафика и т.д. На выходе аналитик информационной безопасности, обслуживающий UBA-системы, будет иметь предупреждения об аномальном поведение конкретных пользователей, с оценкой риска такого поведения и подробными данными, объясняющими что в поведении пользователя является аномалией, когда это началось и как часто повторялось. Все эти данные позволят еще на раннем этапе пресечь многие попытки нарушения информационной безопасности, а также провести качественные расследования уже случившихся инцидентов информационной безопасности.

Со временем на рынке появился модернизированный класс UBA-систем, называемый UEBA-системами (User and Entity Behavior Analytics) — поведенческая аналитика пользователей и ИТ-сущностей. Причиной появления UEBA-систем стал тот факт, что разработчики и специалисты по информационной безопасности осознали, что анализа только поведения пользователей недостаточно для выявления всех возможных атак и самых хитроумных инсайдеров. Принцип действия этого класса систем очень похож на UBA-системы — это глубокий поведенческий анализ, в котором наравне с поведением пользователей анализируется данные об активности различных ИТ-сущностей, таких как АРМ конечных пользователей, сервера, бизнес-приложения, базы данных, учетные записи и другие. Источники входных данных для UEBA-систем в целом аналогичны UBA-системам.

Таким образом, UBA и UEBA-системы очень похожи между собой, но все же кардинально различаются в одном аспекте: UBA-системы акцентируются на пользователях и аномалиях в их поведении, а все данные об ИТ-инфраструктуре являются лишь дополнением для выявления поведенческих аномалий пользователей. UEBA-системы ИТ-сущности рассматривают наравне с пользователями и соответственно строит модели их нормального поведения, что позволяет UEBA-системам обнаруживать самые изощренные и незаметные угрозы информационной безопасности предприятия.

2.1. Задачи, решаемые системами анализа поведения

UBA и UEBA-системы решают следующие основные задачи:

- Анализ в режиме реального времени огромного разнородного массива данных из множества источников для динамического изменения текущего уровня риска пользователей и ИТ-сущностей;
- Оперативное обнаружение атак и инцидентов информационной безопасности, пропускаемых большинством других средств информационной безопасности;
- Ретроспективный анализ данных о случившихся атаках и инцидентах, включающий расширенную информацию обо всех объектах, затронутых в ходе этих событий.

2.2. Сценарии использования

Типовые сценарии использования UBA и UEBA-систем можно разделить на четыре категории:

- Обнаружение скомпрометированных учетных записей;

- Обнаружение скомпрометированных устройств;
- Выявление инсайдеров;
- Ретроспективное расследование нарушений информационной безопасности.

Легальных пользователей информационных систем компании, чьи учетные данные были похищены, почти невозможно обнаружить классическими средствами информационной безопасности. Злоумышленник, выдавая себя за легального пользователя (особенно актуально в случае компрометации административных учетных записей ИТ-персонала), может нанести серьезный ущерб компании и остаться необнаруженным, так как с точки зрения большинства систем информационной безопасности не будут нарушены никакие правила. Такие скомпрометированные учетные записи могут использоваться злоумышленником длительное время, однако использование UBA/UEBA-систем позволит оперативно обнаружить скомпрометированную учетную запись, так как даже самый изощренный и осведомленный злоумышленник не сможет в точности воспроизвести поведение конкретного пользователя, а значит будет выявлено большое количество аномалий относительно нормального поведения пользователя и сгенерировано предупреждение о возможном нарушении информационной безопасности. Наиболее характерными аномалиями в случае компрометации учетных записей пользователей могут выступать необычное время активности (например, после окончания рабочего дня или в выходные, хотя пользователь, как правило, был неактивен в такое время), место подключения (например, при удаленном подключении к ресурсам организации с ip-адресов другой страны), наличие нескольких одновременных сессий и другие. Отдельного внимания заслуживают служебные учетные записи: зачастую они имеют слишком широкие полномочия, но при этом за ними не ведется совершенно никакого контроля. Системы анализа поведения позволят отследить ситуации, при которых подобные учетные записи начнут вести себя подобно пользователям, например, обращаться к каким-то файлам, активно использовать внешнее сетевое подключение и прочие аномалии явно нарушающие типичную активность служебной учетной записи.

С устройствами, которые были скомпрометированы, ситуация обстоит похожим образом. Система анализа поведения выявляет ситуации, когда на таких устройствах появляется нехарактерная активность. Самым ярким примером компрометации устройства может служить использование необычных сетевых протоколов и портов, а также в целом резко выросший объем как внешних, так и внутренних сетевых взаимодействий.

Другой важной проблемой любой организации являются инсайдеры. Они могут долгое время оставаться незамеченными и приносить компании крупные финансовые убытки. UBA/UEBA-системы позволяют обнаруживать такие аномалии, как нехарактерный перебор файлов в поисках ценной информации, открытие бизнес-приложений, не требующихся для непосредственной работы данного пользователя, большие объемы передачи информации во внешний сегмент сети и прочие злоупотребления, которое невидимы для большинства средств защиты информации.

Еще одним важным сценарием использование UBA/UEBA систем является ретроспективное расследование нарушений информационной безопасности. При уже случившемся нарушении, UBA/UEBA система предоставит исчерпывающие данные для специалистов информационной безопасности, занимающихся расследованием инцидента: будут показаны не только объекты, участвовавшие в инциденте, но и взаимодействия между ними, что позволит выявить незамеченные детали и полностью локализовать последствия инцидента, а также не допустить повторения таких инцидентов в будущем.

2.3. Перспективы систем анализа поведения

UBA/UEBA-системы позволяют решать задачи, с которыми не могли справиться традиционные системы защиты информации и аналитики, работающие без помощи интеллектуальных систем. Системы анализа поведения не только предоставляют уже достоверную и полную информацию о нарушениях информационной безопасности, но, в зависимости от настройки, могут обнаруживать даже потенциальные нарушения, которые еще только могут произойти. Все это возможно благодаря анализу в реальном времени огромного количества разнородных данных от множества источников с применением технологий машинного обучения и традиционной статистики.

Немаловажным фактором применения таких систем является возможность проведения ретроспективных расследований нарушений информационной безопасности, при которых будет восстановлена вся картина случившегося, а значит не останется незамеченных уязвимостей, что не позволит нарушению повториться снова.

При всех достоинствах UBA/UEBA-систем, их эффективная работа невозможна полностью без аналитиков-людей. UBA/UEBA-систем тоже способны допускать ложные срабатывания в случаях, когда сотрудник начинает выполнять новые, нехарактерные для себя обязанности сильно отличающиеся от нормальной модели его поведения. В таком случае, аналитику придется самому разобраться в ситуации и убедиться, что сотрудник

действительно выполняет новые должностные обязанности, а не совершает противоправные действия.

Таким образом, UBA/UEBA-системы являются крайне полезными средствами в борьбе с внутренними нарушителями и неизвестными типами угроз, но даже при использовании самых передовых методов машинного обучения, они не могут функционировать полностью без участия человека. Даже самая передовая на данный момент разработка в области искусственного интеллекта не даст того же понимания контекста события информационной безопасности, что и человек. Поэтому UBA/UEBA-системы должны рассматриваться как инструмент, помогающий аналитикам информационной безопасности выявлять и оперативно реагировать на различные аномалии в поведении пользователей и активности ИТ-инфраструктуры, которые могут оказаться действиями злоумышленников, но при этом быть пропущенными другими системами защиты информации.

3. Примеры систем

3.1. Exabeam Advanced Analytics

Exabeam по праву можно считать пионером UBA-рынка. В основе Exabeam Advanced Analytics лежит собственная технология, названная Statefull User Tracking, которая в полностью автоматическом режиме строит нормальный профиль пользователей, опираясь на информацию о сессиях, устройствах, IP-адресах и учетных записях пользователей. Exabeam Advanced Analytics может разворачиваться как в качестве отдельного решения, так и как часть Exabeam Security Intelligence Platform.

К дополнительным задачам, решаемым с помощью платформы Exabeam, можно отнести:

- Инсайдерские угрозы и утечка данных.
- Обнаружение вредоносных программ и их горизонтального распространения.
- Проведение аудита системы на соответствие требованием регуляторов.

3.2. Splunk UBA

Одним из UBA решений стал продукт Splunk UBA, который выпускается как отдельное приложение, построенное на продуктах Big Data Foundation (Hadoop, Spark и GraphDB). Несмотря на это, Splunk UBA имеет прозрачную интеграцию с основным продуктами Splunk Enterprise и Splunk Enterprise Security (SIEM-расширение для платформы Splunk). Splunk UBA создает поведенческие модели пользователей, одноранговых групп, конечных станций, сетевых объектов, источников данных и др.

К дополнительным задачам, решаемым с помощью Splunk UBA, можно отнести:

- Обнаружение кражи интеллектуальной собственности и «эксфильтрация» данных.
- Обнаружение подозрительного поведения в связке пользователей, устройств и приложений.
- Обнаружение вредоносных программ и их горизонтального распространения.

3.3. IBM QRadar UBA

IBM QRadar User Behavior Analytics (UBA) - это приложение для опережающего выявления внутренних угроз. Оно расширяет платформу QRadar Security Intelligence Platform и анализирует шаблоны поведения внутренних пользователей, выявляя идентификационные данные или системы, взломанные злоумышленниками. Приложение отображает пользователей из группы риска на сводной панели, где показаны их имена и аномальные действия, а также инциденты из QRadar. Одним щелчком мыши подозрительный пользователь может быть добавлен в список наблюдения, или его действия могут получить текстовый комментарий. Панель также открывает доступ к данным протокола и текущих событий.

Необходимо отметить, что IBM QRadar UBA является собственной разработкой IBM Security и в планах компании обеспечить непрерывное развитие приложения и расширение сфер его применения.

На сегодняшний день можно выделить несколько дополнительных сфер применения IBM QRadar UBA:

- Определение инсайдерской активности и утечек данных (инициированных пользователями);
- Обнаружение неизвестных угроз и их горизонтального распространения (если такая активность затрагивает конечных пользователей).

3.4. HPE ArcSight UBA

HPE ArcSight UBA — система обеспечения корпоративной безопасности (HPE UBA), дополнительный модуль системы HP ArcSight. Решение позволяет автоматически обнаруживать инциденты информационной безопасности (ИБ) путем профилирования нормальных поведенческих характеристик активности пользователей.

HP UBA помогает решать задачи трех типов:

- анализ любых событий пользовательской активности:
    - доступ к базам данных,
    - файловым каталогам,
    - работа со съемными носителями,

- операции в корпоративных информационных системах (биллинг, платежи, документооборот, работа с персональными данными) и др.

- использование готовых математических моделей по профилированию активности на основе полученных событий:

- группировка однотипных событий (peer group analysis),
- выявление аномалий (anomaly detection),
- определение штатного профиля работы (baseline profiling),
- определение частоты возникновения событий (event rarity).

- применение результатов работы математических моделей к задачам информационной безопасности:

- выявление инсайдеров,
- контроль привилегированных пользователей,
- необычной активности в корпоративных системах
- «спящие счета»,
- «доступ к карточкам ВИП-клиентов».

4. Заключение

В данной статье были проанализированы системы анализа поведения пользователей и ИТ-сущностей, принцип их работы, сценарии использования, а также перспективы применения.

На основании вышеизложенных данных можно сделать следующие выводы:

- UBA/UEBA-системы – довольно эффективное средство выявления скрытых угроз, скомпрометированных учетных записей и внутренних нарушителей;

- UBA/UEBA-системы позволяют обнаруживать аномалии и неочевидные взаимодействия пользователей с корпоративными ресурсами, что позволяет специалистам по информационной безопасности оперативно реагировать на события информационной безопасности и проводить качественные расследования уже свершившихся фактов нарушения информационной безопасности;

- В обозримом будущем отдельные UBA/UEBA-системы или модули с таким функционалом в составе других систем защиты информации станут неотъемлемой частью ежедневной работы сотрудников сферы информационной безопасности.

Список используемых источников

1. Cyber Security Insider “2018 insider threat report” // URL: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (дата обращения: 10.03.2019).
2. Hewlett Packard Enterprise company THE CISO’S GUIDEto Machine Learning & User and Entity Behavioral Analytics // URL: https://www.arubanetworks.com/assets/CisoGuide.pdf (дата обращения: 10.03.2019).
3. Saryu Nayyar Detecting advanced threats with user behavior analytics: https://www.networkworld.com/article/2904356/detecting-advanced-threats-with-user-behavior-analytics.html (дата обращения: 10.03.2019).
4. Обзор рынка систем поведенческого анализа — User and Entity Behavioral Analytics (UBA/UEBA) // URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (дата обращения: 10.03.2019).
5. UEBA, или поведенческая аналитика. Базовая функция всех систем безопасности будущего // URL: http://itsec.ru/articles2/Inf_security/ueba--ili-povedencheskaya-analitika-bazovaya-funktsiya-vseh-sistem-bezopasnosti-buduschego (дата обращения: 10.03.2019).
6. Market Guide for User and Entity Behavior Analytics // URL: https://www.gartner.com/doc/3872885/market-guide-user-entity-behavior (дата обращения: 10.03.2019).
7. Exabeam Advanced Analytics // URL: https://www.exabeam.com/product/exabeam-advanced-analytics (дата обращения: 10.03.2019).
8. Splunk User Behavior Analytics // URL: https://www.splunk.com/en_us/software/user-behavior-analytics.html (дата обращения: 10.03.2019).
9. IBM QRadar User Behavior Analytics // URL: https://www.ibm.com/ru-ru/marketplace/qradar-user-behavior-analytics (дата обращения: 10.03.2019).
10. Splunk User Behavior Analytics // URL: https://www.splunk.com/en_us/software/user-behavior-analytics.html (дата обращения: 10.03.2019).