УДК 002:004.056

АДАПТИВНЫЕ ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ В UEBA-СИСТЕМАХ

А.Ю. Исхаков
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: iay@ipu.ru

Ключевые слова: аутентификация, системы поведенческого анализа, адаптивные системы, DLP, SIEM, UEBA, профиль пользователя, инцидент, OTP пароль, информационная безопасность

Аннотация: В работе рассматриваются общие аспекты построения адаптивной технологии аутентификации, выступающей исполнительным механизмом при возникновении инцидентов, зафиксированных системами интеллектуального контроля и мониторинга. В частности, автором подробно рассматривается класс User and Entity Behavior Analytics систем, представляющих собой интеллектуальный аналитический слой над существующими технологиями безопасности и позволяющих идентифицировать отклонения в поведении пользователей, расставлять приоритеты для зафиксированных инцидентов. Предлагается в качестве реакции на выявленные аномалии в поведении пользователя проводить дополнительную процедуру аутентификации, причем методику дополнительной проверки подлинности подбирать на основе типа выявленной аномалии и заранее построенного профиля конкретного субъекта доступа.

1. Введение

Одним из ключевых факторов, определяющим конкурентоспособность современной системы защиты информации, считается ее способность к целенаправленному приспособлению при изменении компонентов и составных частей защищаемого объекта, технологий обработки информации или условий защиты. Стоит отметить, что далеко не всегда требование к гибкости и адаптируемости механизмов выдвигаются по экономическим соображениям и в связи со значительными затратами на внедрение и обслуживание комплексной системы защиты информации. Зачастую данные модификации продиктованы динамичностью и неопределенностью структуры объекта внедрения. В настоящей работе рассмотрены аспекты реализации адаптивной технологии аутентификации [1], предназначенной для интеграции с системами поведенческого анализа пользователей (User and Entity Behavior Analytics – сокращенно UEBA).

2. Риск-ориентированная аутентификация

Применение традиционных методов парольной аутентификации в качестве единственной системы проверки подлинности субъекта доступа уже давно считается крайне ненадежным способом защиты от злоумышленников. Для снижения рисков компрометации пользовательских учетных записей разработчики повсеместно стараются вне-

дрять решения, основанные на многофакторных алгоритмах проверки подлинности [2]. Однако эта парадигма защиты основана на статических правилах и приводит к строгим ограничениям вне зависимости от личности пользователя и реальных рисков [3]. Ярким примером являются системы дистанционного банковского обслуживания. Традиционно, попытка входа в личный кабинет подобных сервисов сопровождается проверкой OTP-пароля. Данный пароль может быть сгенерирован либо в приложении банк-клиента, либо получен субъектом доступа посредством SMS-сообщения. Подобные процедуры стали обыденной операцией для большинства клиентов, не вызывают значительных затруднений и неудобств при работе в приложении и крайне редко подвергаются критике конечных пользователей.

Однако, клиент должен вводить одноразовый пароль в том числе при подтверждении каждой финансовой транзакции, даже если это регулярный перевод постоянному контрагенту или близкому родственнику. Как правило, политика безопасности финансовой организации предусматривает требование по обязательному выполнению таких процедур вне зависимости от устройства и места, с которого осуществляется вход.

В связи с этим, представители крупных банковских систем активно занимаются поиском решений в области риск-ориентированной аутентификации. Данная концепция подразумевает, что у любого фактора аутентификации есть уровень доверия, а выбор фактора аутентификации зависит от уровня риска конкретной операции. Такие решения безусловно являются крайне важными и актуальными. С одной стороны, они обеспечивают возможность обезопасить клиента от компрометации учетной записи путем анализа активности его профиля на предмет аномальных характеристик, с другой стороны – подобрать баланс между удобством и надежностью, обеспечив в некоторых случаях возможность уменьшить количество процедур аутентификации.

Стоит отметить, что если в случае крупных банковских инфраструктур для вычисления уровней риска событий и уровней доверия факторов аутентификации достаточно задействовать уже установленные решения фрод-мониторинга (используемые во всех каналах банковского обслуживания), то для массового потребителя, как правило, требуется разработка отдельной аналитической подсистемы. Вследствие этого, в качестве интеллектуального механизма по мониторингу активности пользователей предлагается рассмотреть класс UEBA-решений. Данный класс составляют средства автоматизированного анализа поведения пользователя на основании данных журналов доступа для распознавания атак, эффективной приоритезации «срабатываний» различных анализаторов, а также для оказания помощи специалистам по информационной безопасности в эффективном реагировании на угрозы и расследовании инцидентов.

3. Поведенческий анализ в UEBA-системах

Поведенческий анализ пользователей и сущностей как процесс кибербезопасности для детектирования внутренних угроз, атак или мошенничества, обрел высокую популярность среди вендоров и специалистов в сфере информационной безопасности [4]. Причины появления таких решений довольно очевидны. Стремительными темпами увеличиваются объемы информации, циркулирующей в корпоративных сетях, глобальном информационном пространстве. Растет компетенция злоумышленников, а атаки, которые изо дня в день проводятся с целью хищения информации или ее модификации в информационных системах, принимают все более завуалированный вид. Их становится крайне сложно отличить от штатного, легитимного поведения пользователей. Совокупность вышеперечисленных факторов привела к появлению нового класса решений, UEBA-модулей информационной безопасности. В современной литературе выде-

ляется целый ряд различных поднаправлений поведенческого анализа действий пользователей:

- User Behavioral Analytics (UBA);
- Security User Behavior Analytics (SUBA);
- User and Entity Behavior Analytics (UEBA).

Однако, в контексте данного исследования рассматривается наиболее общий класс UEBA-систем, позволяющих дополнять выстраиваемые профили пользователей дополнительными сведениями из системного окружения (системы хранения данных, используемая сетевая инфраструктура, списки приложений и т.д.).

4. Адаптивная аутентификация

На подготовительной стадии, используя алгоритмы машинного обучения, UEBA-сервис определяет типичное поведение для каждого субъекта и ассоциированных приложений. Рассчитываются базовые критерии типичного поведения, отклонения от которого можно измерить. Далее в рамках каждой пользовательской сессии производится постоянный анализ действия каждого субъекта, выполняется сравнивие имеющихся моделей пользовательского профиля с характеристиками выполняемых операций с целью выявления аномального, подозрительного или потенциально рискованного поведения. Обнаружив отклонение, сервис поведенческого анализа запускает интеллектуальную реакцию. В частности, сервис может взаимодействовать с системой регистрации инцидентов и управления ими для сравнения события с аналогичными случаями и предложения целевого решения с участием сотрудника. В дополнение к этому, подобные системы ведут ретроспективную статистику по каждому пользователю и на основе собранных данных по его аномальной активности способны выставлять своеобразные оценки риска каждому из них. В дальнейшем эти оценки используются в ранжировании событий, облегчая работу администратора безопасности.

На рис. 1 представлена схема, характеризующая место выполнения процедур адаптивной аутентификации в рамках традиционной архитектуры UEBA-инструментов, представленной исследователями Gartner [5].

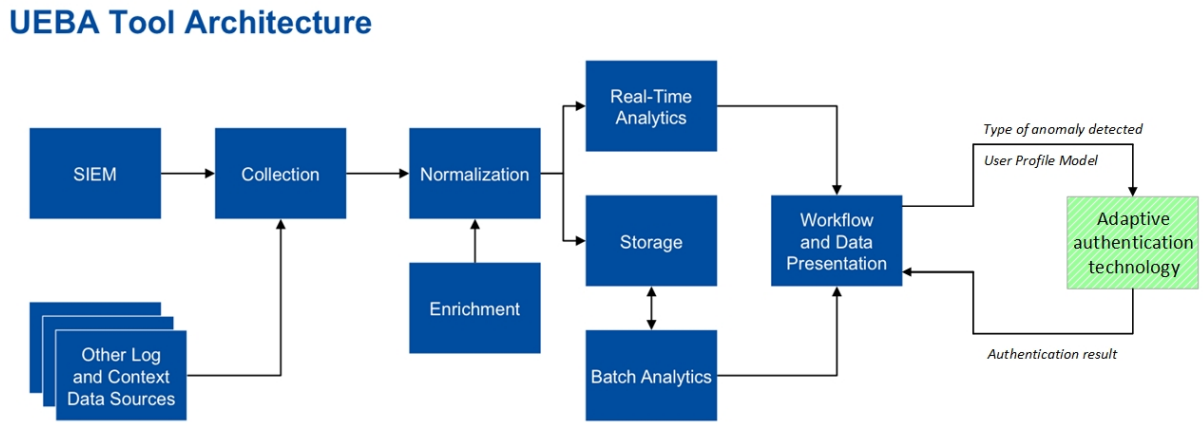

Рис. 1. Применение адаптивной технологии аутентификации в совокупности с UEBA-решениями. В качестве источников могут использоваться нормализованные структуры данных из SIEM-систем и других хранилищ.

Для проведения эффективного анализа UEBA-системы требуют большого количества данных, собранных из разных источников. Чем больше информации о пользователях передается в систему анализа и чем больше приложений оказываются в поле ее зрения, тем выше становится эффективность и скорость выявления фактов подозрительного поведения. Как показано на рисунке 1, задачи сбора и систематизации таких данных решают системы класса Security Information and Event Management (SIEM), предоставляющие доступный в базовых конфигурациях инструментарий по сбору и штатному анализу больших данных. Поэтому наиболее эффективным механизмом внедрения UEBA является их тесная интеграция с уже существующими SIEM-системами [6], которые в свою очередь используют большое число источников данных, обеспечивая максимально полный охват событий, регистрируемых в ИТ- и ИБ-инфраструктуре и приложениях предприятия. Кроме того, производители UEBA-систем, фокусирующихся на внутренних угрозах, в качестве источников информации часто используют не только системные журналы, но и содержание переписок из корпоративной почты и мессенджеров, что позволяет строить более детальные и персонифицированные модели поведения пользователей.

Таким образом, при наличии такого внушительного объема информации появляется возможность интегрировать адаптивную систему аутентификации. Системное свойство адаптивности заключается в способности системы приспосабливаться к изменившимся условиям. В контексте данной работы под адаптивной технологией аутентификации понимается такой набор методов, алгоритмов и научно-технических решений по подтверждению подлинности идентифицируемого субъекта, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, оптимизируя процедуры проверки подлинности путем корректировки наборов факторов, способов, инструментов и критериев аутентификации.

В качестве примера можно рассмотреть следующий сценарий адаптивности процедур аутентификации. Если политика безопасности компании позволяет подключаться к рабочему месту посредством технологии VPN-туннелирования с применением службы удаленного рабочего стола и время от времени сотрудник работает из дома, такой вход в систему не будет отмечен как индикатор риска. При этом, если этот же сотрудник, никогда не бывавший в командировке, вдруг пытается подключиться к системе из другой страны или в нетипичный для его стиля работы временной интервал, система может использовать механизм адаптивного контроля доступа, запустив процедуру двухфакторной аутентификации по одноразовому SMS-паролю.

Рассмотрим другой пример. Помимо внешних атак на инфраструктуру есть большой класс угроз, исходящих от доверенных источников – легитимных сотрудников организации. К числу таких угроз можно отнести утечки данных, внутренний фрод и эксплуатацию уязвимостей в корпоративных системах для повышения привилегий или вывода систем из строя. В подобных случаях UEBA-системы наряду с функционалом Data Loss Prevention (DLP-инструментов) могут своевременно детектировать аномальную активность в поведении пользователей и отреагировать соответствующим образом. Например, при обнаружении нетипичного для конкретного субъекта характера взаимодействия с корпоративными системами (например, экспорта и копирования большого количества конфиденциальных данных) инициировать аутентификацию конкретной операции посредством «механизма доверенных лиц» [7]. Данный механизм может быть реализован в виде запроса разрешения на нетипичную операцию у более привилегированного сотрудника организации.

5. Заключение

Перед индустрией разработок в области автоматизации управления информационной безопасностью компаний стоит множество задач по увеличению эффективности процессов определения и реагирования на инциденты и угрозы. Одну из таких задач решают системы поведенческого анализа. При этом представляется расширение функционала UEBA-инструментов средствами адаптивной аутентификации. Необходимость проверки подлинности, набор и тип факторов, требуемых для аутентификации конкретного субъекта, должны определяться на основе оценки риска угрозы при нетипичном поведении клиента в режиме реального времени.

Важная особенность предложенной технологии адаптивной аутентификации в разрезе задачи обеспечения комплексной информационной безопасности объекта заключается в том, что система UEBA осуществляет постоянный контроль в течение пользовательской сессии (в отличие от традиционных инструментов с однократной проверкой субъекта доступа при входе в систему).

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-01-00767.

Список литературы

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. Исхаков А.Ю., Мещеряков Р.В. Схемы аутентификации пользователя в СКУД с использованием QR кодов и передачи данных по технологии NFC // Информационное противодействие угрозам терроризма. 2014. № 22. С. 11-15.
3. Бродский А. Риск-ориентированная аутентификация // BIS Journal. 2018. № 2 (29). https://journal.ib-bank.ru/post/665
4. Исхаков А. Ю., Исхакова А. О., Мещеряков Р. В., Бендрау Р., Мелехова О. Использование тепловой карты поведения пользователя в задаче идентификации субъекта инцидента информационной безопасности // Труды СПИИРАН. 2018. № 6 (61). С. 147-171.
5. Gartner. UEBA tool architecture. https://www.gartner.com/
6. Матвеев А. Обзор рынка систем поведенческого анализа — User and Entity Behavioral Analytics (UBA/UEBA) // Anti-Malware. https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba
7. Исхаков А.Ю. Методика верификации личности субъекта доступа при удаленной регистрации с помощью доверенных лиц // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. Т. 19, № 3. С. 70-75.