Научная статья
Original article
УДК 004.424

РЕПУТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ВЕБ КОНТЕНТЕ

REPUTATION MODELING IN WEB CONTENT

Кобылко Андрей Эленович, аспирант, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

Kobylko Andrey Elenovich, post-graduate student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

Аннотация. Внутренние угрозы представляют собой серьезную угрозу безопасности любой ИТ-инфраструктуры, включая веб-приложения. Любой сотрудник или третье лицо, имеющее привилегированную или административную учетную запись в веб-приложении, потенциально может повернуться против вас и использовать свой доступ для кражи данных, прерывания операций или допуска других злоумышленников в систему. В статье описаны репутационные методы в вебе.

Annotation. Insider threats are a serious threat to the security of any IT infrastructure, including web applications. Any employee or third party with a privileged or administrative account on your web application could potentially turn against you and use their access to steal data, interrupt operations, or allow other intruders into the system. The article describes reputation methods on the web.

Ключевые слова: Атака, информационная безопасность, веб-контент.

Keywords: Attack, information security, web content.

Внутренние угрозы сложнее выявить или предотвратить, чем внешние атаки, и они невидимы для традиционных решений безопасности, таких как брандмауэры и системы обнаружения вторжений. Эффективная система обнаружения внутренних угроз сочетает в себе несколько инструментов, позволяющих не только отслеживать поведение внутренних пользователей, но и фильтровать большое количество предупреждений и устранять ложные срабатывания.

Инструменты цифровой криминалистики и аналитики, такие как User and Event Behavior Analytics (UEBA), помогают автоматически обнаруживать, анализировать и предупреждать группу безопасности о любых потенциальных внутренних угрозах. Аналитика поведения пользователей может установить базовый уровень для нормального доступа к данным, а мониторинг активности базы данных может помочь выявить нарушения политик.

Поведенческая аналитика пользователей и событий (UEBA) — помогает защититься от внутренних угроз, атак нулевого дня и APT.

Мониторинг активности базы данных — отслеживает реляционные базы данных, хранилища данных, большие данные и мейнфреймы для создания предупреждений в реальном времени о нарушениях политик.

Предотвращение потери данных (DLP) — проверка данных в движении, в состоянии покоя, в облаке или на конечных точках.

Устройства для обмана, такие как ложные цели и приманки, а также мониторинг и аудит использования данных в режиме реального времени.

Большинство кибератак и большинство современных векторов угроз связаны с использованием автоматических ботов . Каждый месяц тысячи ботов поражают присутствие в Интернете, некоторые из них являются законными, другие - вредоносными ботами, которые ищут уязвимости и потенциально используют их. Боты также могут использоваться для

получения доступа к данным организации другими способами, например, путем веб-скрейпинга.

Решения для защиты от ботов могут выявлять и блокировать плохих ботов, а хорошим ботам разрешать доступ к сайту.

Профили поведения — профилирование поведения трафика с течением времени для выявления пользователей-людей, хороших и плохих ботов.

Анализ репутации — ведение базы данных сигнатур ботов и определение того, соответствует ли текущий трафик известным плохим ботам.

Вызовы — заголовки HTTP/S, подписи IP и ASN, вызовы cookie и JavaScript, чтобы определить, являются ли боты, поражающие сайт, законными или вредоносными.

Существует несколько подходов и инструментов для обеспечения безопасного управления доступом. Если у вас нет полной системы управления идентификацией и доступом (IAM), решение для обеспечения безопасности должно предоставлять автоматизированный способ обеспечения многофакторной аутентификации, помогать вам отфильтровывать плохой трафик с известных вредоносных IP-адресов или других вредоносных источников, позволяя вам для определения пользовательских политик для выборочной блокировки или пропуска трафика.

Многофакторная проверка подлинности — передовые решения для обеспечения безопасности могут помочь вам применять многофакторную проверку подлинности всякий раз, когда кто-либо входит в веб-приложение, не требуя внесения изменений в базовое приложение.

Управление репутацией — может фильтровать трафик на основе обнаружения таких источников, как анонимные прокси, сеть TOR или подозрительные географические регионы.

Черный список IP -адресов — определяет известные источники плохого трафика и использует их для блокировки плохих запросов и управления репутацией.

Из-за серьезности внутренних угроз и сложности выявления и блокировки внутренней атаки превентивной мерой является предотвращение захвата учетной записи. Решения для захвата учетных записей используют процесс обнаружения на основе намерений для выявления злонамеренных входов в систему с использованием поведенческого анализа и данных глобальной аналитики угроз.

Обнаружение на основе намерений — выявляет вредоносные входы в систему посредством перекрестной проверки репутации и поведения, классификации клиентов и т. д.

Наблюдение за активностью входа в систему — позволяет просматривать активность входа в систему по всему предприятию, видеть, подвергаются ли сайты атакам, определять, какие учетные записи пользователей были взломаны и что было сделано с учетными данными.

Аналитика угроз — передовые решения используют глобальную базу данных шаблонов атак, сопоставляя ее с шаблонами входа в среду с помощью машинного обучения.

Многие веб-приложения предоставляют API, что позволяет другим участникам цифровой экономики использовать веб-приложение в автоматическом режиме. API-интерфейсы становятся все более важными и сложными, но обычно не защищаются и не контролируются должным образом. Многие API-интерфейсы не были созданы с учетом надежных методов обеспечения безопасности и могут позволять пользователям вводить вредоносные данные или иным образом неправомерно использовать API.

Безопасность API защищает конечные точки API, отслеживая запросы API и обеспечивая доступ к конечной точке только проверенному правильному трафику.

Конечные точки API должны быть защищены, как только они будут опубликованы, и безопасность должна быть частью процесса разработки. Расширенные решения позволяют создавать определения безопасности с использованием стандарта OpenAPI, поэтому вы можете встроить

безопасность в свой API по мере его разработки и публиковать его с автоматически применяемыми параметрами безопасности.

Блокируйте нежелательный трафик — перехватывайте и блокируйте трафик с известных плохих IP-адресов, подозрительных регионов, анонимных прокси, сети TOR и т. д.

Аналитика атак — передовые решения могут обнаруживать и блокировать известные шаблоны атак с помощью брандмауэра веб-приложений (WAF).

Защита от DDoS- атак уровня 3/4 — защищает API-интерфейсы от DDoS-атак, как на сетевом уровне (например, Synflood), так и на уровне приложений.

Интеграция со шлюзом API. Решения для обеспечения безопасности API должны интегрироваться с распространенными шлюзами API, такими как Azure, AWS или RedHat.

Решения для обеспечения безопасности веб-сайтов часто развертываются на границе сети и принимают решения о трафике, поступающем на веб-сайт. Настройка необходима для того, чтобы решение для обеспечения безопасности не нарушило бизнес: если решение блокирует законный трафик, оно может нанести такой же ущерб, как и атаки, для предотвращения которых оно предназначено.

Убедитесь, что решение для обеспечения безопасности не нарушит бизнес — определите настраиваемые правила для управления автоматическим реагированием, реагированием на определенные атаки, включите определенные варианты использования.

Ведущие поставщики систем безопасности имеют опыт защиты тысяч организаций и защитили от миллионов атак. Ищите решение, которое дает вам доступ к группе безопасности поставщика и дает вам аутсорсинговую помощь для определения политик и конфигурации безопасности, а также для решения повседневных инцидентов безопасности.

Основным преимуществом наличия под рукой исследовательской группы по безопасности является защита от угроз нулевого дня. У организаций, оперирующих только собственными интеллектуальными данными, очень мало шансов защититься от угроз нулевого дня. Могут пройти недели или месяцы, прежде чем об угрозе станет известно, будут выпущены исправления, и они будут фактически развернуты в локальных ИТ-системах.

С группой исследователей безопасности на стороне поставщика, как только угроза нулевого дня становится достоянием общественности или как только одна организация подвергается угрозе, шаблон атаки распространяется на всех пользователей инструмента безопасности. Все они могут быть защищены мгновенно путем развертывания новой конфигурации безопасности, блокирующей угрозу.

Аналитики безопасности от поставщиков помогают анализировать предупреждения и устранять ложные срабатывания.

Группы реагирования на инциденты, предлагаемые поставщиком

Большинство организаций сталкиваются с хронической нехваткой сотрудников службы безопасности и взрывным ростом предупреждений, связанных с безопасностью, от множества инструментов. Аналитика поведения пользователей и сущностей (UEBA) может быть важным инструментом для определения приоритетов оповещений и обеспечения того, чтобы специалисты по безопасности рассматривали только те оповещения, которые действительно представляют вредоносную активность.

Технология UEBA устанавливает базовый уровень поведения для учетных записей пользователей, конечных точек и объектов в сети, таких как коммутаторы, маршрутизаторы и приложения. Оповещение генерируется только тогда, когда активность отклоняется от этого базового уровня и превышает допустимый порог.

Ключевая особенность:

Поведенческая аналитика - выявляйте реальную вредоносную активность с помощью UEBA, чтобы уменьшить количество ложных срабатываний.

Аналитика угроз - сопоставьте шаблоны трафика с известными сигнатурами атак, чтобы идентифицировать атаки и предоставить информацию о субъектах угроз.

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.
2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.

4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Кобылко А.Э., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.

Для цитирования: Кобылко А.Э. РЕПУТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ВЕБ КОНТЕНТЕ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.